



POWERING ACTIONABLE INTELLIGENCE®

# Nextiva S4300 Series User Guide

---

Covering the S4300, S4300-BR, and  
S4300-RP

Firmware Release 5.30

April 2009

© 2009 Verint Systems Inc. All Rights Reserved Worldwide.

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Verint Systems Inc. is strictly prohibited. By providing this document, Verint Systems Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice. Features listed in this document are subject to change.

Verint Systems Inc. does not warrant, guarantee or make any representation regarding the use or the results of the use of the information, links, tools, and materials in terms of the accuracy, reliability, quality, validity, stability, completeness, currentness, or otherwise of its content or products. The entire risk as to the use, results and performance of information, links, tools and materials provided or referenced herein is assumed by the user. Verint Systems Inc. shall not be liable for damages resulting from the use, misuse or unlawful use of the information, links, tools, and materials contained or referenced herein.

The Verint Systems Inc. products are protected by one or more of the following U.S., European or International Patents: USPN 5,659,768; USPN 5,689,442; USPN 5,790,798; USPN 6,278,978; USPN 6,370,574; USPN 6,404,857; USPN 6,510,220; USPN 6,724,887; USPN 6,751,297; USPN 6,757,361; USPN 6,782,093; USPN 6,839,667; USPN 6,952,732; USPN 6,959,078; USPN 6,959,405; USPN 7,047,296; USPN 7,149,788; USPN 7,155,399; USPN 7,203,285; USPN 7,216,162; USPN 7,219,138; USPN 7,254,546; USPN 7,281,173; USPN 7,284,049; USPN 7,325,190; USPN 7,466,816; USPN 7,478,051; USPN RE40,634; and other provisional rights from one or more of the following Published US Patent Applications: US 11/394,408; US 11/771,499; US 11/396,514; US 11/772,440; US 11/565,943; US 11/565,946; US 11/565,948; US 11/540,739; US 11/540,086; US 11/541,313; US 11/541,252; US 11/540,282; US 11/529,947; US 11/540,785; US 11/540,736; US 11/540,904; US 11/540,353; US 11/608,340; US 11/608,350; US 11/608,358; US 11/567,808; US 11/692,983; US 11/693,933; US 11/693,923; US 11/693,828; US 11/567,852; US 11/608,440; US 12/015,621; US 11/540,322; US 11/924,201; US 11/616,490; US 11/621,134; US 11/752,458; US 11/712,933; US 11/824,980; US 11/729,185; US 11/804,748; US 11/831,260; US 11/395,992; US 11/359,319; US 11/359,195; US 11/359,357; US 10/832,509; US 11/742,733; US 11/831,257; US 11/831,250; US 11/691,530; US 11/479,267; US 11/529,942; US 11/768,349; US 11/540,281; US 10/633,357; US 11/693,899; US 11/479,056; US 11/529,132; US 11/540,320; US 11/037,604; US 11/529,842; US 11/540,171; US 11/478,714; US 11/529,946; US 11/868,656; US 11/776,659; US 11/090,638; US 11/410,004; US 10/771,315; US 10/771,409; US 11/540,900; US 11/528,267; US 12/118,781; and other U.S. and International Patents and Patents Pending.

VERINT, the VERINT logo, ACTIONABLE INTELLIGENCE, POWERING ACTIONABLE INTELLIGENCE, WITNESS ACTIONABLE SOLUTIONS, STAR-GATE, RELIANT, VANTAGE, X-TRACT, NEXTIVA, ULTRA, AUDIOLOG, WITNESS, the WITNESS logo, IMPACT 360, the IMPACT 360 logo, IMPROVE EVERYTHING, EQUALITY, CONTACTSTORE, and CLICK2STAFF are trademarks or registered trademarks of Verint Systems Inc. or its subsidiaries. Other trademarks mentioned are the property of their respective owners.

[www.verint.com/videosolutions](http://www.verint.com/videosolutions)

Publication date: April 2, 2009

Publication revision: C

# Contents

<b>Preface</b> .....	<b>vii</b>
<b>Chapter 1 ■ Overview</b> .....	<b>1</b>
About the S4300 Series .....	2
Key Features .....	2
Security .....	3
Installation Kit .....	3
S4300 Model .....	3
S4300-BR Models .....	4
S4300-RP Model .....	5
Hardware Overview .....	6
Hardware Dimensions and Mounting Angles .....	7
Computer Requirements .....	11
<b>Chapter 2 ■ System and RF Planning</b> .....	<b>12</b>
Available Frequency Bands and Channels .....	13
2.4 GHz Band .....	13
4.9 GHz Band .....	13
5 GHz Band .....	15
Wireless Cells .....	16
Roles .....	16
Compatibility Issues .....	17
Video Bit Rate and Data Throughput .....	18
System Planning .....	20
TPC .....	20
DFS .....	20
Application Types .....	22
Access Point .....	23
Point-to-Multipoint Repeater .....	24
Point-to-Point Repeater .....	25
Wireless Bridge .....	26
Wireless Bridge Repeater .....	27
Redundant Master Setup .....	28
Colocated Cells .....	29
Distance Limitations .....	29
4.9 GHz Band in America .....	30
5 GHz Band in America and 2.4 GHz Band .....	31
5 GHz Band in Europe .....	32
False Radar Detection .....	33
Preferred Setups .....	34
Risky Setups .....	35
RF Planning .....	36
Location Evaluation .....	36
Antenna Requirements .....	38
RF Exposure Considerations .....	38
<b>Chapter 3 ■ Configuring and Installing an Access Point</b> .....	<b>39</b>
Presenting the Application .....	40

Connecting Power .....	40
Configuring the System .....	41
Setting Network Parameters .....	42
Setting the Device Name and Country of Operation .....	44
Setting Wireless Parameters .....	44
Checking Communication .....	47
Installing the System .....	48
Mounting a Device on a Pole or Wall .....	48
Installing an External Antenna .....	52
<b>Chapter 4 ■ Configuring and Installing a Wireless Bridge .....</b>	<b>54</b>
Presenting the Application .....	55
Connecting Power .....	56
Power over Ethernet .....	56
12V DC/24V AC Power .....	57
Configuring the System .....	58
Setting Network Parameters .....	58
Setting the Device Name and Country of Operation .....	60
Setting Wireless Parameters .....	61
Checking Communication .....	65
Installing the System .....	65
Mounting a Device on a Pole or Wall .....	65
Installing an External Antenna .....	70
<b>Chapter 5 ■ Configuring and Installing a Point-to-Point Repeater .....</b>	<b>72</b>
Presenting the Application .....	73
Connecting Power .....	73
Configuring the System .....	74
Changing the IP Address of the Computer .....	74
Setting Network Parameters .....	77
Setting the Device Name and Country of Operation .....	79
Setting Wireless Parameters .....	80
Checking Communication .....	83
Installing the System .....	84
Mounting a Device on a Pole or Wall .....	84
Installing an External Antenna .....	88
<b>Chapter 6 ■ Configuring and Installing a Point-to-Multipoint Repeater .....</b>	<b>90</b>
Presenting the Application .....	91
Connecting Power .....	91
Configuring the Application .....	92
Setting Network Parameters .....	93
Setting the Device Name and Country of Operation .....	95
Setting Wireless Parameters .....	95
Checking Communication .....	98
Installing the System .....	99
Mounting a Device on a Pole or Wall .....	99
Installing an External Antenna .....	103
<b>Chapter 7 ■ Configuring and Installing a Wireless Bridge Repeater .....</b>	<b>105</b>
Presenting the Application .....	106
Connecting Power .....	106
Configuring the Application .....	107
Setting Network Parameters .....	108

Setting the Device Name and Country of Operation .....	110
Setting Wireless Parameters .....	110
Checking Communication .....	113
Installing the System .....	114
Mounting a Device on a Pole or Wall .....	114
Installing an External Antenna .....	118
<b>Chapter 8 ■ Using the Web Interface .....</b>	<b>120</b>
Installing or Upgrading ActiveX Controls .....	121
Viewing the Quick Status .....	122
Configuring the Device .....	124
Configuring Access Management .....	125
User Accounts .....	125
Security .....	126
Viewing the System Status .....	128
Configuring the Network .....	129
Configuring Wireless Communication .....	130
Basic Wireless .....	130
Advanced Wireless .....	133
Configuring VSIP .....	135
Configuring System Time .....	136
Configuring HTTP (Webserver) .....	138
Maintaining the Device .....	139
<b>Chapter 9 ■ Maintaining and Troubleshooting the Device .....</b>	<b>142</b>
Updating the Firmware .....	143
Detecting a Duplicate Master .....	143
Finding a “Lost” S4300 .....	143
Performing a Reset .....	144
Recognizing the LED Conditions .....	144
Using the Command Line Interface .....	147
Accessing the CLI .....	147
Configuring Quality of Service .....	149
Selecting a Frequency Channel .....	149
<b>Appendix A ■ Factory Default Configuration .....</b>	<b>150</b>
<b>Appendix B ■ DHCP Support and APIPA .....</b>	<b>152</b>
<b>Appendix C ■ Surge Protection .....</b>	<b>154</b>
12V/24V Power .....	155
External Antenna .....	155
Ethernet Port .....	155
<b>Appendix D ■ RF Contact between Masters .....</b>	<b>158</b>
<b>Appendix E ■ Reducing Wireless Interference .....</b>	<b>161</b>
Interference from External Sources .....	162
Interference from Nextiva Devices .....	162
Performing a Site Survey .....	163
Respecting Minimum Distances .....	167
<b>Appendix F ■ Technical Specifications .....</b>	<b>170</b>
<b>Glossary .....</b>	<b>173</b>
<b>Index .....</b>	<b>178</b>

**Compliance .....183**

    USA ..... 184

    Canada ..... 186

    Mexico ..... 188

    Europe ..... 190

    RoHS Declaration of Compliance ..... 192

# Preface

The *Nextiva S4300 Series User Guide* presents the information and procedures on installing and configuring the Nextiva® S4300 series multipurpose outdoor wireless device. The series includes:

- S4300—A single device for access point applications
- S4300-BR—Two devices for wireless bridge applications
- S4300-RP—Two devices for repeater applications

## Audience

This guide has been prepared for the following audience:

- Managers
- IT system administrators
- Engineers
- Technicians

This guide assumes that you are familiar with:

- Installation and manipulation of electronic equipment
- General use of computers
- Local area networks (LANs) and basic IP data communication concepts and practices
- Radio frequency (RF) platforms
- Web browsers
- Microsoft Windows operating systems

## Reference

In addition to this guide, the following documentation is also available:

- *Nextiva S4300 Installation Guide*
- *Nextiva S4300-BR Installation Guide*
- *Nextiva S4300-RP Installation Guide*
- *Verint SConfigurator User Guide*
- *Nextiva S4X00 Release Notes*

A paper copy of the installation guide is included with your order.

## How to Contact Us

The following Web sites and e-mail addresses provide information and support for Verint Video Solutions and the Nextiva Intelligent Edge Device product line.

Find general information on Verint Video Solutions, including marketing material and product information at [www.verint.com/videosolutions](http://www.verint.com/videosolutions).

Find general information on Verint Video Solutions, including marketing material and product information at [www.verint.com/videosolutions](http://www.verint.com/videosolutions).

Download the documentation of the Intelligent Edge Devices at [www.verint.com/manuals](http://www.verint.com/manuals).

Download firmware from the Verint Video Solutions partner extranet at <http://vvs.verint.com>.

Send your questions or comments on the current document, or any other Nextiva user documentation, to our documentation feedback team at [documentationfeedback@verint.com](mailto:documentationfeedback@verint.com).

Find contact information for the Verint Customer Service team, by phone or e-mail, or fill out a Web request for support with a specific issues at [www.verint.com/videoservice](http://www.verint.com/videoservice). For immediate assistance, contact the Customer Service team:

Location	Telephone	E-mail
USA and Canada	1-888-747-6246	vissupport@verint.com
Central and Latin America	+1-631-962-9202	vissupport@verint.com
Europe, Middle East, and Africa	+44 (0) 845-843-7333	customersupport.emea@verint.com
	+49 (0) 4321-269 81 36	mobilesupport@verint.com (Transit applications only)
Asia/Pacific		APAC_VIS_Services@verint.comp
Hong Kong	+852 2797 5678	
Singapore	+65-68266099	



# 1

## Overview

The S4300 series is a multipurpose, outdoor, wireless, digital video product covering the 2.4 GHz and 5 GHz frequency bands in America (United States, Canada, and Mexico) and Europe, and the 4.9 GHz public safety band in America.

Note: The S4300 series devices require professional installation.



The overview covers the following:

- About the S4300 Series
- Installation Kit
- Hardware Overview
- Hardware Dimensions and Mounting Angles
- Computer Requirements

# About the S4300 Series

The S4300 series has many uses, namely:

- Access point application—A communication hub for multiple S4200 series devices
- Point-to-point repeater—A range extender for one or many pairs of S4100 series devices
- Point-to-multipoint repeater—A range extender for multiple S4200 series devices
- Wireless bridge—A link between two networks (wired or wireless)
- Wireless bridge repeater—A range extender for a wireless bridge

To cover these application types, the following S4300 models are available:

- S4300—A single device for access point applications
- S4300-BR—Two devices for wireless bridge applications
- S4300-RP—Two devices for repeater applications

Input power varies depending of the model:

Model	12V DC or 24V AC	Power over Ethernet (PoE)
S4300		✓
S4300-BR	✓	✓ (S4300-BR-PoE)
S4300-RP	✓	

You can also purchase each device for the 4.9 GHz public safety band (the suffix *-49* is added to the product name, for example *S4300-BR-49*).

Unless otherwise specified, the word *S4300* refers to any of these devices.

## Key Features

The S4300 offers the following key features:

- Integration of a multiband radio and antenna into small outdoor rated enclosures, for convenient, discreet, secure, and reliable installation in real-world video security applications
- Integrated antenna covering the 2.4 GHz (8.5 dBi), 4.9 GHz (12 dBi), and 5 GHz (12 dBi) bands
- Multipurpose outdoor device that can be used as an access point, point-to-point repeater, point-to-multipoint repeater, wireless bridge, or wireless bridge repeater
- Ethernet port for configuring the device or connecting an IP camera on an S4300-BR
- Web interface for easy configuration
- NTP (Network Time Protocol) support

- Wireless MAC/protocol enhancements specific to wireless video security applications
- Resolution of limitations of standard WiFi technology for wireless video security applications (hidden nodes, latency, range, and QoS)
- Low-latency communication to avoid problems such as PTZ over control

## Security

Every S4300 device comes with the following security features:

- **SSL**—Every edge device comes with a unique SSL (Secure Sockets Layer) certificate for securing its IP link. SSL is a commonly used protocol for managing the security of IP message transmission. If enabled, the SSL protocol secures the VSIP communication data. It does not apply to audio and video transmission.
- **SPCF**—The SmartSight Point Coordination Function proprietary protocol resolves the “hidden node,” quality of service, range, and security problems. SPCF is used in access point applications and in repeater contexts. With this protocol, a master S4300 has total control over the radio frequency used; therefore, in an RF line-of-sight context, two cells cannot share the same frequency channel.

## Installation Kit

The package contents vary depending on the S4300 model. For each model, you can purchase external high-gain antennas.

**Note:** You must use only antennas certified by Verint. Doing so ensures that the combined transmission power of the device and antenna does not exceed the maximum value established by your country's regulations. For more information, see page 28 and page 183.

## S4300 Model

The package contents for an S4300 model are:

Item	Description
Access point	One S4300 access point; includes an integrated antenna
Mounting assembly set	One set for installation on a wall or pole
Power-over-Ethernet (PoE) kit	48V DC 802.3af PoE injector and power cord
Outdoor Ethernet cable	An 82-foot (25-meter) outdoor Ethernet cable with a weatherproof connector
Printed material	The <i>Nextiva S4300 Installation Guide</i>

Item	Description
<b>Options</b>	
High-gain antenna	One external antenna; the available antennas vary depending on the frequency band and the country.
CABET-25 cable	An 82-foot (25-meter) outdoor Ethernet cable with a weatherproof connector
CABET-50 cable	A 164-foot (50-meter) outdoor Ethernet cable with a weatherproof connector

## S4300-BR Models

The wireless bridge can be powered with PoE (S4300-BR-PoE) or 12V DC (S4300-BR).

The package contents for an S4300-BR-PoE model are:

Item	Description
Wireless bridge	S4300-BR consisting of two devices. Each device includes an integrated antenna.
Mounting assembly set	Two sets for installation on a wall or pole
Power-over-Ethernet (PoE) kit	Two 48V DC 802.3af PoE injectors and power cords
Outdoor Ethernet cable	Two 82-foot (25-meter) outdoor Ethernet cables with a weatherproof connector
Printed material	The <i>Nextiva S4300-BR Installation Guide</i>
<b>Options</b>	
High-gain antenna	One or two external antennas; the available antennas vary depending on the frequency band and the country.
CABET-25 cable	An 82-foot (25-meter) outdoor Ethernet cable with a weatherproof connector
CABET-50 cable	A 164-foot (50-meter) outdoor Ethernet cable with a weatherproof connector

The package contents for an S4300-BR model are:

Item	Description
Wireless bridge	S4300-BR consisting of two devices. Each device includes an integrated antenna.
Mounting assembly set	Two sets for installation on a wall or pole
Power cable	Two cables for 12V DC or 24V AC power
Outdoor Ethernet cable	Two 82-foot (25-meter) outdoor Ethernet cables with weatherproof connectors
Printed material	The <i>Nextiva S4300-BR Installation Guide</i>
<b>Options</b>	
High-gain antenna	One or two external antennas; the available antennas vary depending on the frequency band and the country.
PS2440 power supply	An indoor-only 24V AC power supply
CABET-25 cable	An 82-foot (25-meter) outdoor Ethernet cable with a weatherproof connector
CABET-50 cable	A 164-foot (50-meter) outdoor Ethernet cable with a weatherproof connector
CABPV cable	A cable for 12V DC or 24V AC power

## S4300-RP Model

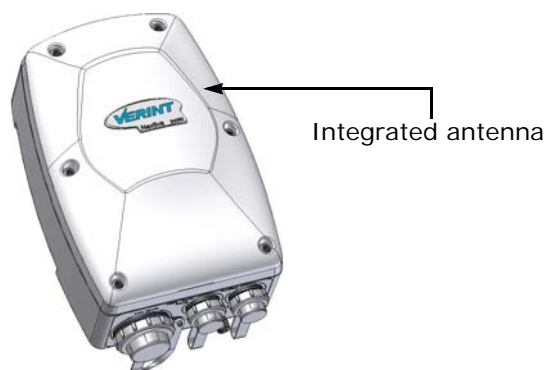
The package contents for an S4300-RP model are:

Item	Description
Repeater	S4300-RP consisting of two devices. Each device includes an integrated antenna.
Mounting assembly set	Two sets for installation on a wall or pole
Power cable	Two cables for 12V DC or 24V AC power
Outdoor Ethernet cable	One 6-foot (2-meter) outdoor Ethernet cable
Printed material	The <i>Nextiva S4300-RP Installation Guide</i>

Item	Description
<b>Options</b>	
High-gain antenna	One or two external antennas; the available antennas vary depending on the frequency band and the country.
PS2440 power supply	An indoor-only 24V AC power supply
CABET-25 cable	An 82-foot (25-meter) outdoor Ethernet cable with a weatherproof connector
CABET-50 cable	A 164-foot (50-meter) outdoor Ethernet cable with a weatherproof connector
CABPV cable	A cable for 12V DC or 24V AC power

## Hardware Overview

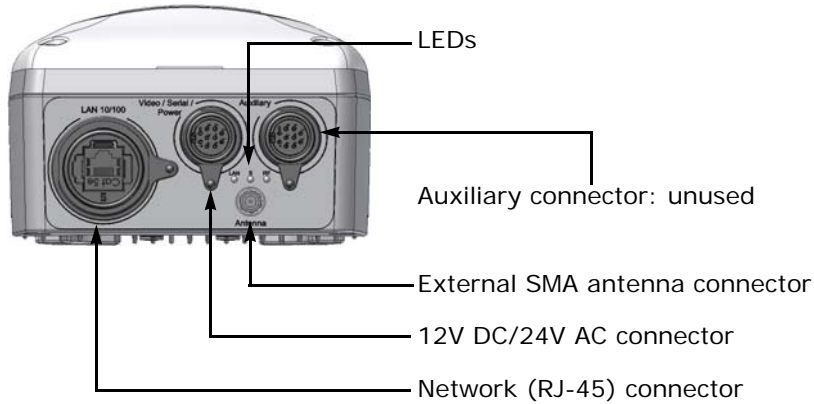
The S4300 electronics are enclosed in a weather-tight cast aluminum module with an integrated wide-band antenna located in the top of the casing. All cable entries are mounted on the underside of the module to maintain its weatherproof properties.



The underside consists of:

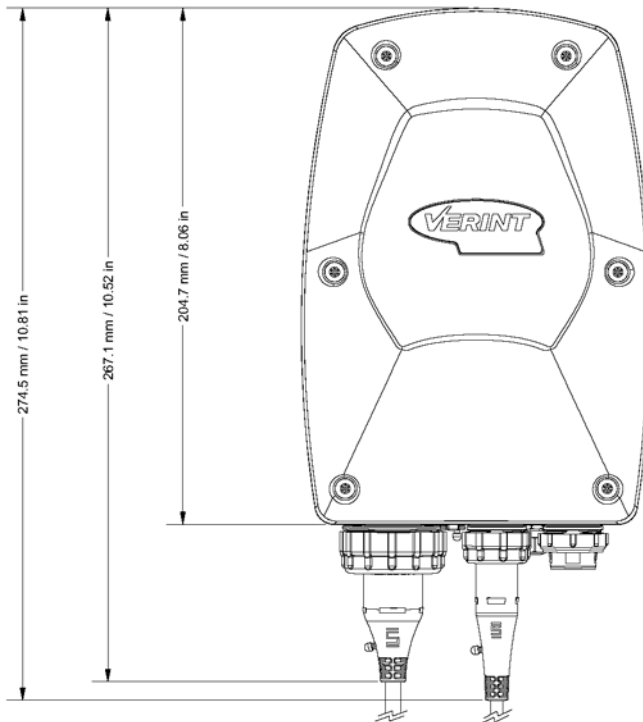
- A network (RJ-45) connector
- A 12V DC/24V AC power connector
- An auxiliary connector (unused)
- An external SMA antenna connector

■ Three LEDs

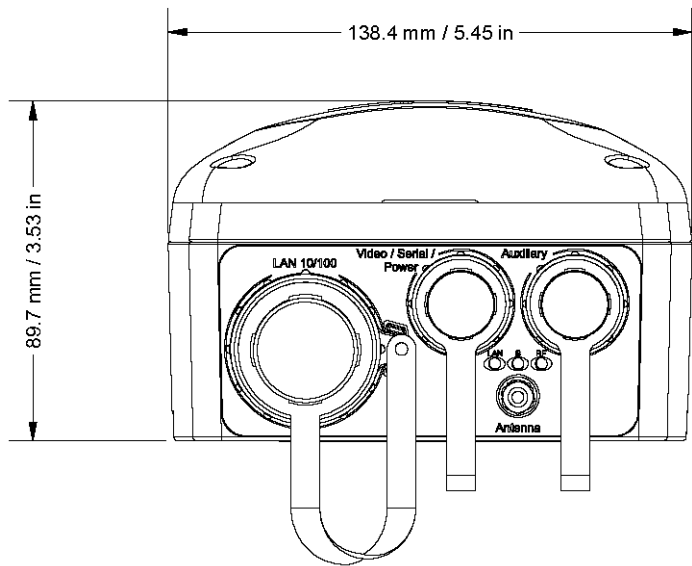


## Hardware Dimensions and Mounting Angles

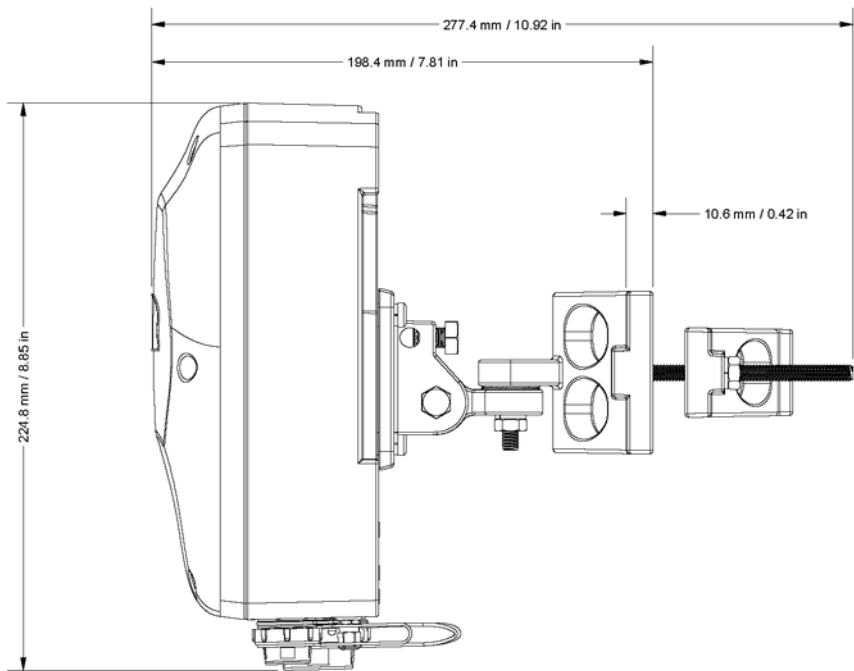
The top view dimensions of the S4300 are:



The back view dimensions are:

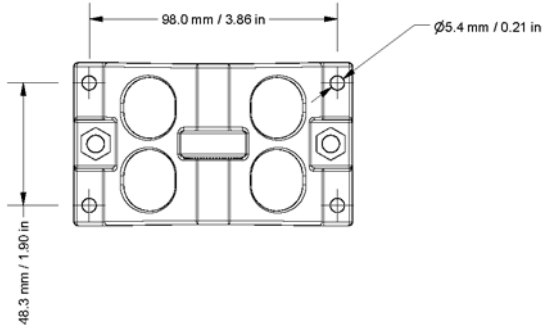


The side view dimensions with the mounting assembly installed are:

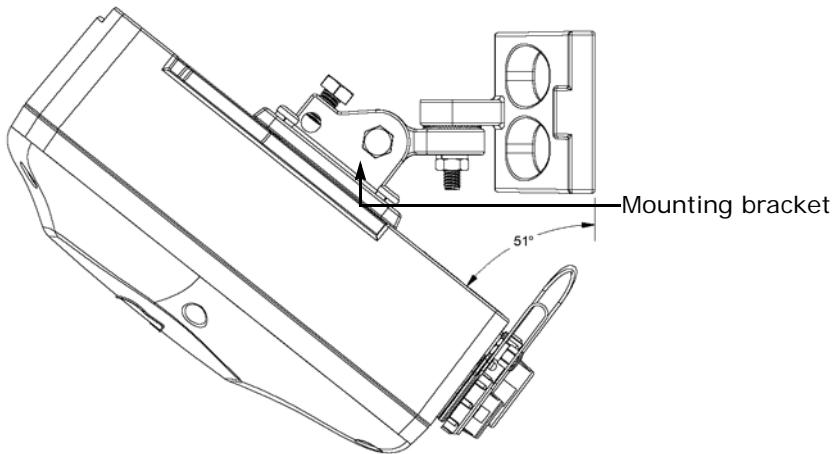




The dimensions of the wall pivot mount are:

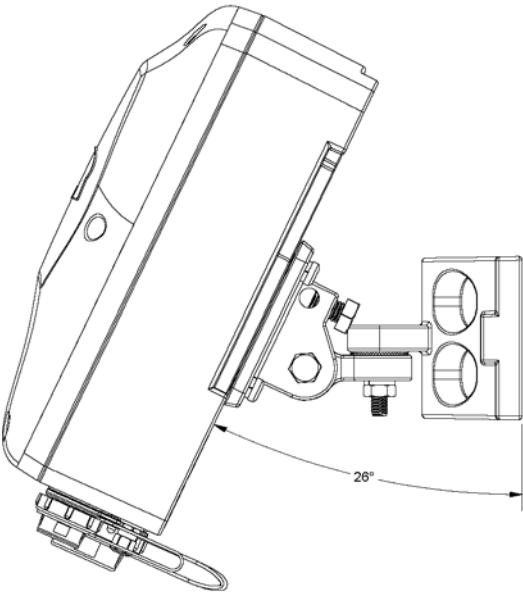


The maximum angular positions allowed by the mounting bracket vary depending on the cables and the mounting structure (pipe, wall, and so on). Here is a downward tilt:



To cover more installation possibilities, you can install the mounting bracket upside down in order to flip all the angles; for instance, to provide a downward tilt the same maximum angle as an upward tilt. For more information about the mounting procedure, see the "Installing the System" section in the configuration chapter of the S4300 model you purchased.

An upward tilt is:



Finally, here are rotation examples:

Left Rotation	Right Rotation
A technical line drawing of a camera unit mounted on a bracket. The camera is rotated to the left from a central reference line. An arc indicates the angle of rotation, which is labeled as 64°.	A technical line drawing of a camera unit mounted on a bracket. The camera is rotated to the right from a central reference line. An arc indicates the angle of rotation, which is labeled as 84°.

# Computer Requirements

The minimum hardware and software requirements for the host computer needed to configure the edge device are:

- An Ethernet network card
- Internet Explorer 6.0 or higher
- Microsoft DirectX 8.1 or higher
- Windows 2000 Service Pack 2 or higher, or Windows XP Service Pack 2 or higher

# 2

## System and RF Planning

To allow optimal configuration, you must properly plan your network, especially configuration layout and RF (radio frequency). Planning is especially required if you want to install many systems in the same area, in order to prevent radio interference between the colocated devices and to select the appropriate antennas. In all cases, follow the recognized RF installation practices.

To help you with your planning, you may consult the Verint Video Intelligence Solutions extranet:

- The *Wireless System Margin Calculator* is a tool based on an Excel spreadsheet designed to simplify the creation of RF systems. It is located under Tools.
- The *Nextiva Wireless Devices Primer* provides standardized information about the design, features, and benefits of the Nextiva wireless devices. It is located under Community Links > Technical Briefs > Nextiva Intelligent Edge Devices.

The system and RF planning tasks cover the following topics:

- Available frequency bands and channels
- Wireless cells
- System planning
- Application types
- Colocated cells
- RF planning

# Available Frequency Bands and Channels

The S4300 supports communications in the following frequency bands in America and Europe:

- 2.4 GHz OFDM, also known as 802.11g
- 4.9 GHz OFDM, a public safety band available in the United States and Canada only
- 5 GHz OFDM, also known as 802.11a

To meet local regulations, you must use only antennas that conform to the requirements specified in the “Compliance” appendix on page 183.

## 2.4 GHz Band

The 2.4 GHz band provides 11 channels in the United States, Canada, and Mexico, and 13 in Europe. In these two regions, only channels 1, 6, and 11 are independent (that is, non-overlapping); in most countries, they can be used indoors or outdoors. For more information on the availability of these channels depending on the countries, see the “Compliance” appendix on page 183. The center frequencies of the channels are:

Channel	Frequency (GHz)	Channel	Frequency (GHz)
1	2.412	8	2.447
2	2.417	9	2.452
3	2.422	10	2.457
4	2.427	11	2.462
5	2.432	12	2.467 (Europe only)
6	2.437	13	2.472 (Europe only)
7	2.442		

## 4.9 GHz Band

The 4.9 GHz band is a licensed band for entities providing public safety services focused on the protection of life, health, or property in the United States, Canada, and Mexico. This band provides license holders with an interference-free, secure channel for robust and secure broadband technologies, including wireless video surveillance systems.

For more detailed information concerning the regulations governing licensing and use of frequencies in the 4.9 GHz band:

- United States—See Subpart Y of the FCC document, Memorandum Opinion and Order and Third Report and Order at:  
[http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-03-99A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-99A1.pdf)
- Canada—See the document SP-4940 (Spectrum Utilization Policy, Technical and Licensing Requirements for Broadband safety in the band 4940-4990) at:  
<http://strategis.ic.gc.ca/epic/site/smt-gst.nsf/en/sf08667e.html>
- Mexico—The use of the 4.9 GHz in Mexico is subject to a special approval from COFETEL.

The 4.9 GHz band has a width of 50 MHz (4940 to 4990 MHz). Since the standard channel width is 20 MHz, only two independent channels can co-exist in the band. However, the S4300 supports channel fragmentation, allowing narrower channels of 5 MHz and 10 MHz. You can have up to four independent channels with a 10 MHz width, and up to 10 with a 5 MHz width. All these channels are for indoor or outdoor use.

The available channels are:

Channel	Frequency (GHz)	Channel Width
3	4.9425	5 MHz
6	4.9475	5 MHz
7	4.9525	5 MHz or 10 MHz
7	4.950	20 MHz
8	4.9575	5 MHz
9	4.9625	5 MHz or 10 MHz
10	4.9675	5 MHz
11	4.9725	5 MHz or 10 MHz
11	4.970	20 MHz
12	4.9775	5 MHz
13	4.9825	5 MHz or 10 MHz
16	4.9875	5 MHz

## 5 GHz Band

In the 5 GHz band, the number of available channels and sub-bands vary depending on the country of operation.

Most European countries adhere to the DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control) regulations established by the European Telecommunications Standards Institute (ETSI); these regulations apply to the 5 GHz frequency band only. To know which bands are available in your country of operation and whether your country adheres to DFS and TPC, see the “Compliance” appendix on page 183.

In the United States and Canada, five channels are available in the 5 GHz band, all independent and for indoor or outdoor use. The center frequencies of these channels are:

Channel	Frequency (GHz)
149	5.745
153	5.765
157	5.785
161	5.805
165	5.825

In Mexico, the following channels are available, all independent and for indoor or outdoor use:

Channel	Frequency (GHz)	Channel	Frequency (GHz)
36	5.18	64	5.32
40	5.2	149	5.745
44	5.22	153	5.765
48	5.24	157	5.785
52	5.26	161	5.805
56	5.28	165	5.825
60	5.30		

In Europe, the 11 independent channels, for indoor or outdoor use, are:

Channel	Frequency (GHz)	Channel	Frequency (GHz)
100	5.50	124	5.62
104	5.52	128	5.64
108	5.54	132	5.66
112	5.56	136	5.68
116	5.58	140	5.70
120	5.60		

## Wireless Cells

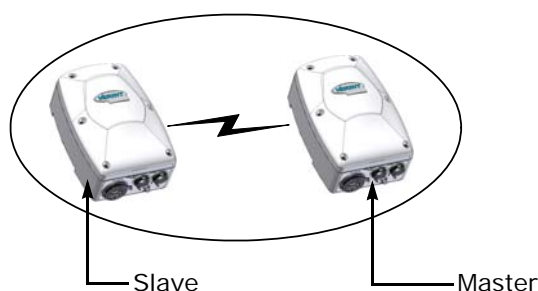
A wireless network is designed such that information can travel back and forth between two points without the need for wires. Wireless devices are grouped into *wireless cells*. The devices in a cell communicate together on the same frequency channel and share the same wireless passkey.

## Roles

An S4300 can have two MAC (Media Access Control) roles, according to its function in the wireless cell, master or slave:

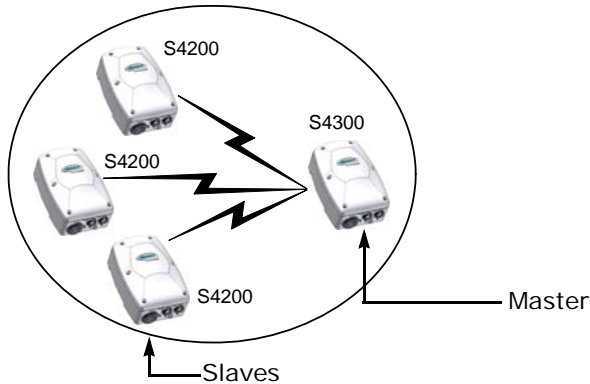
- A master device controls the access over the wireless medium. It takes care of channel selection and slave authentication to provide access to the wireless network. Finally, the master allocates bandwidth among all connected slaves.
- Slave devices need a master to access the wireless medium to transfer data, through a polling mechanism. Also, the other wireless devices (S4100, S4200) that can be connected to S4300 devices are slaves.

In this first example of a wireless cell, two S4300 devices, a master and a slave, form a wireless bridge:





The second example shows three slaves associated to an S4300 master device:



You can colocate many wireless cells if you respect certain conditions (see page 29).

## Compatibility Issues

When planning your wireless systems, you need to take into account the firmware versions of the involved devices. It is recommended that the S4300 devices have the same firmware versions as their associated slaves. Furthermore, you can use the S4300 with S1100w transmitters at firmware version 4.12 or higher.

In a wireless cell involving S4200 transmitters, the order in which you configure the devices (either the first time or later when they are installed in the field) or update their firmware is critical if you do not want to lose access to them:

1. Update or configure the devices starting with the farthest (in terms of number of RF hops) from the computer running the procedure.
2. One step at a time, get closer to the host computer.

In a point-to-point repeater:

1. Update the firmware of all S4100 pairs, starting with the remote device.
2. Change the IP address of the computer running SConfigurator.
3. Update the firmware of the two S4300 devices.

For example, consider the following wireless cell:



Update or configure the devices in the following order:

1. S4200 1—You then lose contact with S4200 1.
2. S4200 2—You then lose contact with S4200 2.
3. S4300 1—You can then reach all devices.
4. S4300 2—You then lose contact with all devices except master S4300 3.
5. S4300 3—You can then reach all devices.

For the complete firmware update procedure, refer to the *Verint SConfigurator User Guide*.

## Video Bit Rate and Data Throughput

You can theoretically connect up to 24 slave devices to a master S4300 in a wireless cell. In practice however, video quality, frame rate, and system layout can limit the number of devices that a single master can support.

Available video data throughput can be evaluated using the Wireless System Margin Calculator that you can find on the Verint extranet. Available video data throughput depends on the transmission (tx) bit rate used by each slave on the wireless network.

Video quality and frame rate also influence the required data throughput. Therefore, you need to carefully plan the number of cameras that will work on a link.

The following figures were measured in typical setup situations (with the SPCF MAC protocol). They may vary depending on your configuration. The total data throughput in a unidirectional UDP link setup varies depending on the frequency channel width: 20 MHz in all available bands, or 5 MHz and 10 MHz in the 4.9 GHz frequency band.

The throughput for a 20 MHz channel is:

Physical Bit Rate	Throughput for a 3-Mile (5 km) Distance	Throughput for a 9.3-Mile (15 km) Distance	Throughput for a 15.5-Mile (25 km) Distance
6 Mbps	5.1 Mbps	5.1 Mbps	5.0 Mbps
9 Mbps	7.3 Mbps	7.3 Mbps	7.2 Mbps
12 Mbps	9.5 Mbps	9.5 Mbps	9.4 Mbps
18 Mbps	13.4 Mbps	13.3 Mbps	13.1 Mbps
24 Mbps	16.8 Mbps	16.7 Mbps	16.4 Mbps
36 Mbps	22.0 Mbps	22.0 Mbps	21.9 Mbps
48 Mbps	26.3 Mbps	25.5 Mbps	25.0 Mbps
54 Mbps	28.1 Mbps	27.1 Mbps	26.0 Mbps

The throughput for a 10 MHz channel is:

Physical Bit Rate	Throughput for a 3-Mile (5 km) Distance	Throughput for a 9.3-Mile (15 km) Distance	Throughput for a 15.5-Mile (25 km) Distance
3 Mbps	2.3 Mbps	2.3 Mbps	2.3 Mbps
4.5 Mbps	3.8 Mbps	3.7 Mbps	3.7 Mbps
6 Mbps	5.0 Mbps	4.9 Mbps	4.9 Mbps
9 Mbps	7.2 Mbps	7.1 Mbps	7.1 Mbps
12 Mbps	9.3 Mbps	9.3 Mbps	9.2 Mbps
18 Mbps	12.9 Mbps	12.8 Mbps	12.6 Mbps
24 Mbps	16.0 Mbps	15.8 Mbps	15.5 Mbps
27 Mbps	17.2 Mbps	16.9 Mbps	16.7 Mbps

The throughput for a 5 MHz channel is:

Physical Bit Rate	Throughput for a 3-Mile (5 km) Distance	Throughput for a 9.3-Mile (15 km) Distance	Throughput for a 15.5-Mile (25 km) Distance
1.5 Mbps	1.3 Mbps	1.3 Mbps	1.3 Mbps
2.25 Mbps	2.0 Mbps	2.0 Mbps	2.0 Mbps
3 Mbps	2.5 Mbps	2.5 Mbps	2.5 Mbps
4.5 Mbps	3.7 Mbps	3.6 Mbps	3.6 Mbps
6 Mbps	4.7 Mbps	4.6 Mbps	4.6 Mbps
9 Mbps	6.8 Mbps	6.7 Mbps	6.7 Mbps
12 Mbps	8.5 Mbps	8.5 Mbps	8.4 Mbps
13.5 Mbps	9.5 Mbps	9.4 Mbps	9.3 Mbps

The S4300 automatically adjusts the transmission speed with the current RF conditions.

# System Planning

The grouping of devices in each wireless cell is determined by their respective locations with respect to one another and by the available S4300 devices. As a rule of thumb, each slave device must have a clear RF line of sight with its master device within each cell. However, the slaves can be completely hidden from one another. For more information about the RF line of sight, see page 36.

The system planning aspects to consider are:

- TPC
- DFS
- Application types
- Redundant master setup

## TPC

If the country of operation of the S4300 device requires conformity to the TPC (Transmit Power Control) rules, the maximum EIRP (effective isotropic radiated power) is reduced by 3 dBm from the allowed maximum value; for example, if the maximum EIRP is 30 dBm in the band and region of operation, the maximum EIRP in the device will be set to 27 dBm.

The combined transmission power of the device and its antenna must not exceed this maximum value. For that reason, you must specify the antenna gain during configuration; the device will automatically take it into account and adjust its own transmission power accordingly at startup. This adjustment is done in all wireless devices (masters and slaves).

To meet local regulations, you must use only antennas that conform to the requirements specified in the “Compliance” appendix on page 183.

## DFS

In countries following the DFS (Dynamic Frequency Selection) regulations, frequency channel selection is performed by the master device. Frequency channel selection can be automatic (default) or manual; manual selection allows a better RF planning.

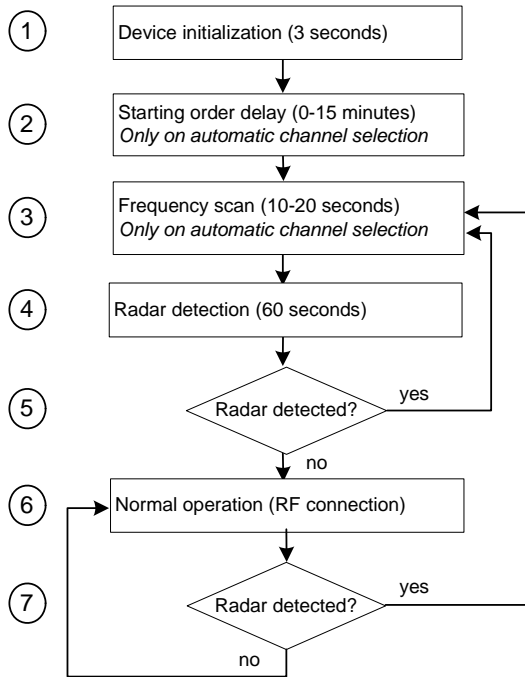
**Note:** DFS is required only in the 5 GHz band.

The radar detection mechanism (including channel availability check and non-occupancy period) can be performed on all wireless devices (master and slave); it also allows for **better RF planning and optimal wireless network performance**. The procedure is the same regardless of the type of frequency channel selection.

**Note:** To minimize the false radar detection problem in colocated systems using adjacent frequency channels, see page 33.

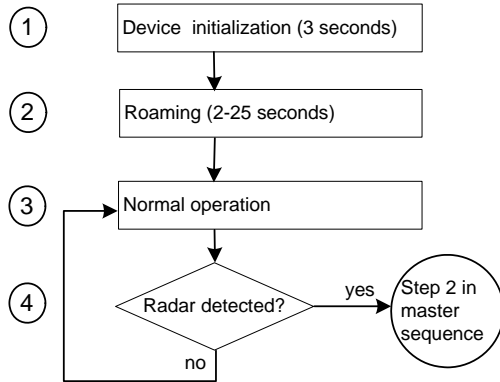
You should start the master first, then power the slave when the other device is in normal operation.

A master device in DFS mode goes through the following sequence when booting up:



1. The device goes through the standard startup procedure.
2. If automatic channel selection is active, the starting order delay ensures that colocated masters will not select a frequency channel at the same time, therefore minimizing the possibility that they choose the same one. For more information about the starting order, see page 134.
3. If automatic channel selection is active, the device scans the available frequencies (based on the selected country) and automatically selects a channel; in the selection process, channels already used by colocated masters will be discarded at first.
4. The device listens for 60 seconds on the selected channel to detect possible radar interference.
5. If a radar is detected on the channel, the device returns to the scan process, even if the channel was manually selected. The manual selection is no longer available: The device will automatically choose another frequency channel. It will not return to scan the channel in which the radar was detected for the next 30 minutes. If no radar is detected, the device continues its bootup procedure.
6. The RF connection is established; the device runs normally.
7. If a radar is detected, the device stops transmission on that channel and immediately goes back to the scan process to select another one. It will not return to scan the channel in which the radar was detected for the next 30 minutes.

The boot sequence of slave devices is:



1. The device goes through the standard startup procedure.
2. The device roams through the channels in the available frequency bands to locate its master; it does not transmit any data.
3. When the master is located, the slave runs normally on the selected frequency channel.
4. If the slave detects a radar on the channel during normal operation, it informs the master then stops operation. Upon reception of this message, the master starts its radar detection process.

Radar detection on slave devices can be disabled; for more information, see page 33.

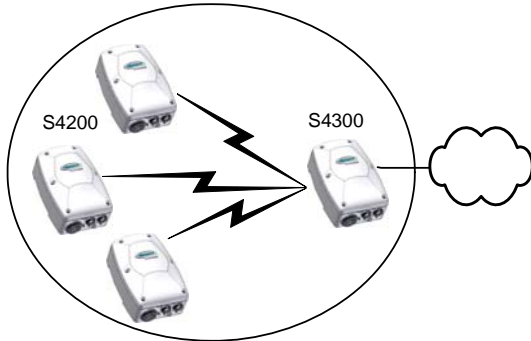
## Application Types

The S4300 devices are used in many types of applications, including:

- Access point—One S4300 device linking multiple S4200 transmitters to a LAN (the S4300 model)
- Point-to-point repeater—Two S4300 devices acting as a range extender for one or many S4100 systems (the S4300-RP model)
- Point-to-multipoint repeater—Two S4300 devices acting as a range extender for multiple S4200 transmitters (the S4300-RP model)
- Wireless bridge—Two S4300 devices linking two networks, wired or wireless (the S4300-BR model)
- Wireless bridge repeater—Two S4300 devices acting as a range extender for a wireless bridge (the S4300-RP model)

## Access Point

An access point application is a wireless cell made up of an S4300 device (the S4300 product code, called the *master*) and several S4200 transmitters (the *slaves*). Here is a typical access point system:



To install a single wireless cell made up of three S4200 transmitters and one S4300, you need to:

1. Assign the same wireless passkey to the S4200 and S4300 devices.
2. In a non-DFS context or in a DFS context with manual frequency channel selection, assign a frequency channel to the S4300.

The associated S4200 transmitters will automatically use their master's channel.

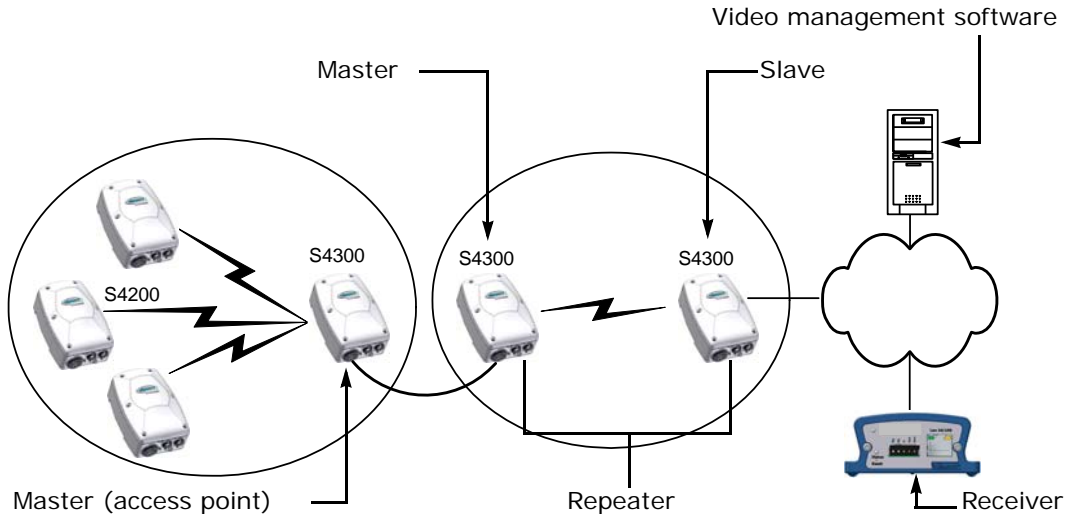
3. Install the S4200 transmitters such that each one has a clear RF line of sight with the S4300 device.

For the complete configuration and installation procedures, see page 39.

## Point-to-Multipoint Repeater

A point-to-multipoint repeater is used as a range extender for wireless links to retransmit the signals coming from S4200 transmitters towards the Ethernet LAN. A typical context is when you cannot obtain an RF line of sight between the transmitters and the S4300 connected to the wired LAN.

A point-to-multipoint repeater (the S4300-RP product code) is made up of two S4300 devices; the application also needs an S4300 access point. Two colocated cells are required; for example:



To operate the two cells forming the repeater, you need to:

1. In each cell, assign the same wireless passkey to all the devices. The wireless passkey must be different from that of the other cell.
2. Always connect the S4200 transmitters to a master S4300, never to a slave.
3. In a non-DFS context or in a DFS context with manual frequency channel selection, assign a frequency channel to the master S4300 device in each cell. For better isolation, use different frequency bands.
4. In a DFS context with automatic channel selection, set a different starting order for each master S4300. Ensure that the two masters see each other.
5. Install the S4200 and slave S4300 devices such that each one has a clear RF line of sight with its associated master.

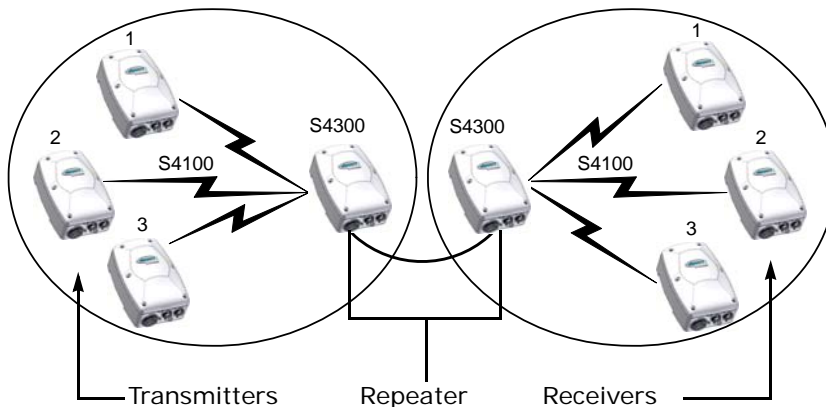
For the complete configuration and installation procedures, see page 90.



## Point-to-Point Repeater

A point-to-point repeater is used as a range extender for wireless links to retransmit the signals coming from one or many S4100 transmitters to their corresponding receivers. A typical context is when you cannot obtain an RF line of sight between the transmitters and the receivers.

A point-to-point repeater (the S4300-RP product code) is made up of two master S4300 devices, separated into two colocated cells. For example, with three pairs of S4100 devices:



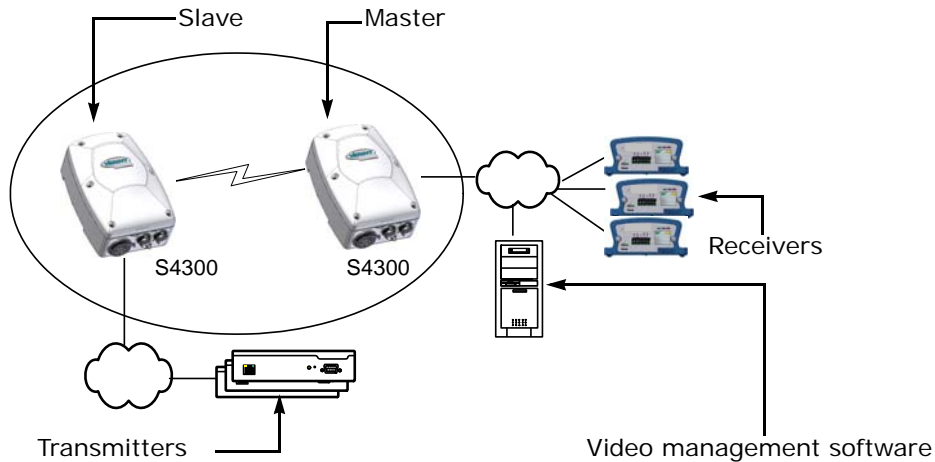
To operate the two cells forming the repeater, you need to:

1. In each cell, assign the same wireless passkey to all the devices. The wireless passkey must be different from that of the other cell.
2. In a non-DFS context or in a DFS context with manual frequency channel selection, assign a frequency channel to the master S4300 device in each cell. For better isolation, use different frequency bands.
3. In a DFS context with automatic channel selection, set a different starting order for each master S4300. Ensure that the two masters see each other.
4. Install the S4100 devices such that each one has a clear RF line of sight with its associated master.

For the complete configuration and installation procedures, see page 72.

## Wireless Bridge

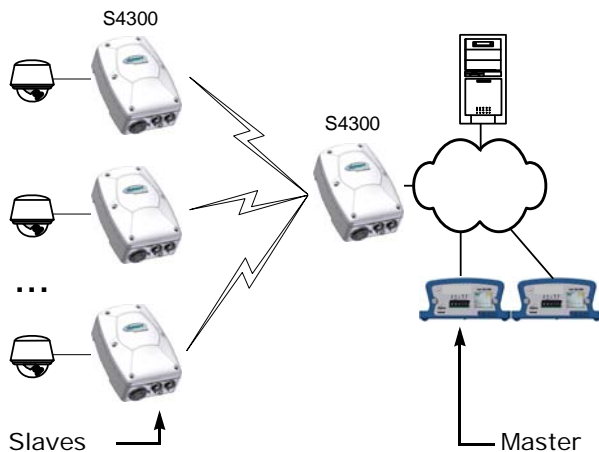
You use two S4300 devices (the S4300-BR product code)—a master and a slave—to transfer video surveillance data between two LANs when a wired connection is not available or too costly to install. For instance, a wireless bridge application can connect remote S1900e-AS edge devices (the following illustration) or wireless devices without an RF line of sight.



To create a wireless bridge application, you need to:

1. Assign the same wireless passkey to the two S4300 devices.
2. In a non-DFS context or in a DFS context with manual frequency channel selection, assign a frequency channel to the master S4300 device.
3. Install the S4300 devices such that there is a clear RF line of sight between them.

You can also use the S4300-BR product in point-to-multipoint wireless bridges, to transmit video coming from IP cameras:



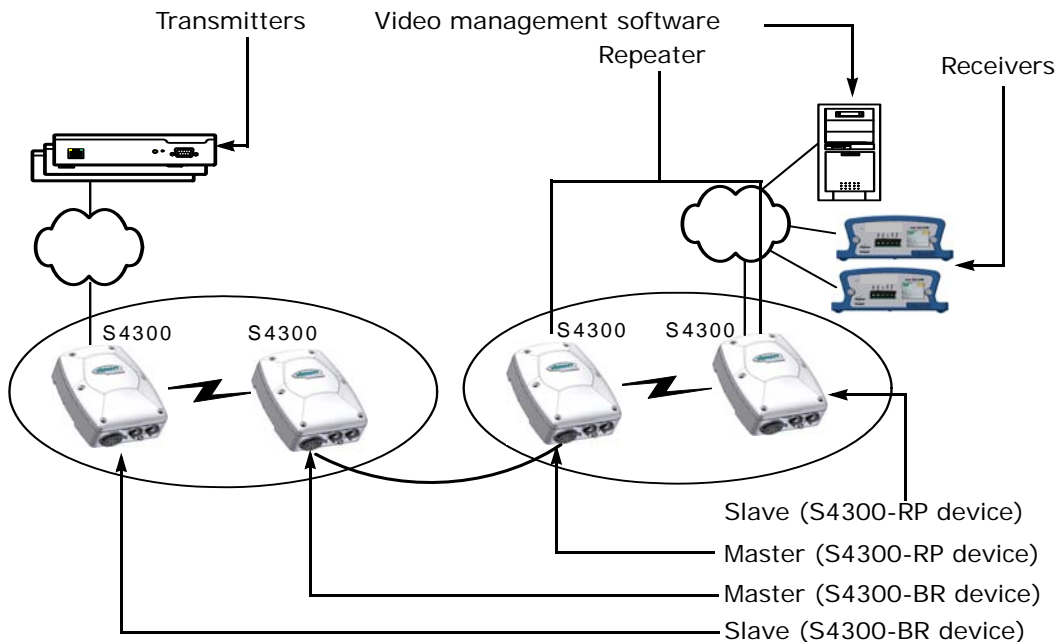
All slaves (you can install up to 24 of them) must be S4300-BR devices. See “Video Bit Rate and Data Throughput” on page 18 for the considerations when connecting many slaves to the same master. The configuration of such an application is very similar to that of a standard wireless bridge.

For the complete configuration and installation procedures, see page 54.

### Wireless Bridge Repeater

A wireless bridge repeater is used as a range extender to retransmit the signals exchanged by the two devices forming a wireless bridge. A typical context is when you cannot obtain an RF line of sight between the two devices forming the wireless bridge.

A wireless bridge repeater (the S4300-RP product code) is made up of two devices; the application also needs an S4300-BR bridge. Two colocated cells are required; for example:



To operate the two cells forming the repeater, you need to:

1. In each cell, assign the same wireless passkey to the two devices. The wireless passkey must be different from that of the other cell.
2. In a non-DFS context or in a DFS context with manual frequency channel selection, assign a frequency channel to the master S4300 device in each cell. For better isolation, use different frequency bands.
3. In a DFS context with automatic channel selection, set a different starting order for each master S4300. Ensure that the two masters see each other.
4. Install the S4300 series devices such that each one has a clear RF line of sight with its corresponding counterpart.

For the complete configuration and installation procedures, see page 105.

## Redundant Master Setup

It is possible to organize your system such that a master S4300 takes over the management of a wireless cell when a nearby master fails (power or wireless failure). This failover mechanism works for S4300 master devices in any type of applications (access points, wireless bridges, and repeaters).

**Tip:** If there is a complete loss of video in a redundant system, check the communication on the Ethernet network and the network connectivity on the master S4300.

Proper RF planning is required to ensure that the wireless system does not suffer degraded video performances. Ensure that your system meets the following conditions:

- The masters must share the same wireless passkey.
- The masters must have different frequency channels from the same frequency band.
- The two frequency channels should not be adjacent and be used by other wireless cells in close vicinity. For more information, see “Colocated Cells” on page 29.
- The masters must be part of the same network.
- The total data throughput required by all the slaves must not exceed the total available throughput on a single master. For example, if your total throughput is 28 Mbps per master, do not set up your slaves such that they generate a total of 40 Mbps (two times 20 Mbps).
- The antennas of the masters must point in the same direction.
- The slaves are located in the central beam width of the antennas of the two masters.

Slaves automatically switch to the redundant master. As soon as the main master fails, the slaves start their roaming process to find another master; they will connect to the redundant master because it uses the same wireless passkey and is in the same frequency band.

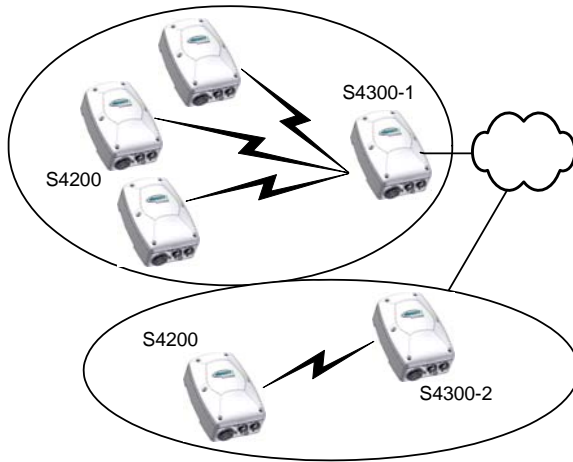
Failover time is dependent on the RF roaming capabilities of the wireless slave devices. The time it takes for a slave to connect to the redundant master depends on the number of channels the slaves are required to scan and the total number of slaves in the wireless cell. In an environment free of interference, all slaves should reconnect to the redundant master within 60 seconds of RF connectivity loss.

In a redundant setup, the slaves can be split between the two masters, therefore creating two wireless cells. It is during its initial roaming process that each slave finds a master sharing the same wireless passkey; therefore it can connect to any of the two masters. This situation is perfectly normal and does not prohibit the proper behavior of the redundant masters.

**Note:** Remember that the goal of a redundant system is to ensure that there will be no performance degradation and data loss in case a master fails. Therefore, design your redundant system as though you have only one master, not two.

Since you have no control over the split of slaves between the masters, organize your system in such a way that there will be enough bandwidth if all slaves are connected to a single master.

In the following access point example, the three S4200 transmitters connected to S4300-1 will be able to connect to S4300-2 if their master fails:



To test a redundant master setup, follow these steps:

1. Install and configure all the devices.
2. Disconnect the power of a master. Check that all the slaves connect to the other master.
3. Repeat step 2 for the second master.

## Colocated Cells

You can operate many wireless cells in the same location, provided you follow guidelines relative to frequency band and channel, wireless passkey, distance, and location.

Two colocated cells cannot use the same frequency channel.

The wireless passkeys of colocated cells must be different from one another, regardless of their frequency channels.

## Distance Limitations

The distance limitations between devices in colocated cells are:

- The minimum distance between two devices is 3 feet (1 meter), regardless of the band or channel used.
- To avoid material damages, you must never power any two devices while their antennas are facing one another with a distance of less than 10 feet (3 meters).
- To reduce radio interference, separate as much as possible devices sharing the same pole or installed on the same roof, even if they do not use adjacent channels.
- If using adjacent channels, see page 167 for the recommendations on the minimum distances to respect.

## 4.9 GHz Band in America

Depending on the channel width (20, 10, or 5 MHz), you can colocate 2, 4, or 10 wireless cells respectively in the United States, Canada, and Mexico. For the available channels in each of the three scenarios, see page 14.

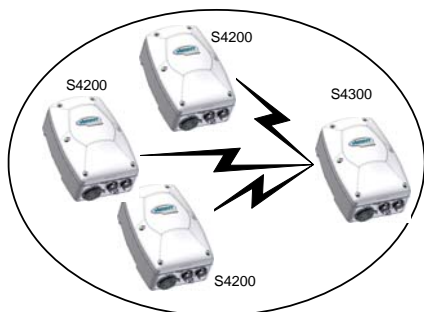
The following example presents three wireless cells with 10-MHz channels. To install such a system, you have to:

1. In each cell, assign the same wireless passkey to the S4200 transmitters and the S4300 access point. The wireless passkey must be different from that of the other cells.
2. Assign a different frequency channel to each S4300 device; the associated S4200 devices will automatically use their master's channel:

Device	Cell	Channel	Wireless Passkey
S4300_A	A	7	ertynmbvcxzapoio
S4200_A1	A	7	ertynmbvcxzapoio
S4200_A2	A	7	ertynmbvcxzapoio
S4200_A3	A	7	ertynmbvcxzapoio
S4300_B	B	13	PUK98rewq4123qzx
S4200_B1	B	13	PUK98rewq4123qzx
S4200_B2	B	13	PUK98rewq4123qzx
S4200_B3	B	13	PUK98rewq4123qzx
S4300_C	C	11	987123jkl456wert
S4200_C1	C	11	987123jkl456wert
S4200_C2	C	11	987123jkl456wert
S4200_C3	C	11	987123jkl456wert

3. In each cell, install the S4200 devices such that each one has a clear RF line of sight with its associated S4300 access point.

This application can be illustrated this way, where the three cells are in the same location:



## 5 GHz Band in America and 2.4 GHz Band

In the 2.4 GHz band in United States, Canada, Mexico, and Europe, you can use the three independent channels (channels 1, 6, and 11) to colocate wireless cells. In the 5 GHz band in the United States, Canada, and Mexico, all channels are independent.

A typical colocation example is three access point applications, each one made up of three S4200 transmitters and one S4300. To install such a system, you need to:

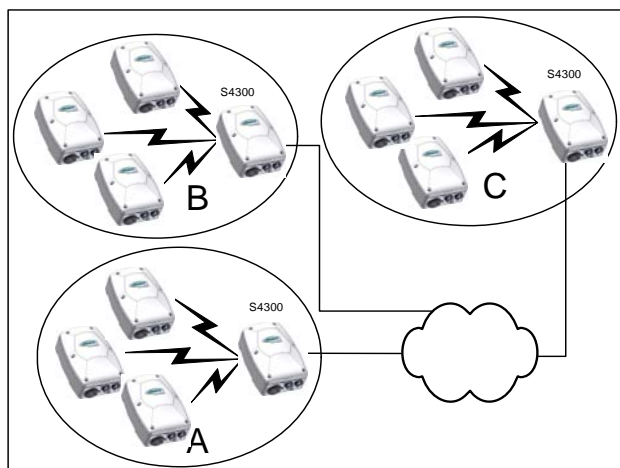
1. In each cell, assign the same wireless passkey to the S4200 transmitters and the S4300 device. The wireless passkey must be different from that of the other cells.
2. Assign a different frequency channel to each S4300 master device; the associated S4200 transmitters will automatically use their master's channel. For example:

Device	Cell	Channel	Wireless Passkey
S4300_A	A	149	ertynmbvcxzapoju
S4200_A1	A	149	ertynmbvcxzapoju
S4200_A2	A	149	ertynmbvcxzapoju
S4200_A3	A	149	ertynmbvcxzapoju
S4300_B	B	165	PUK98rewq4123qzx
S4200_B1	B	165	PUK98rewq4123qzx
S4200_B2	B	165	PUK98rewq4123qzx
S4200_B3	B	165	PUK98rewq4123qzx
S4300_C	C	157	987123jkl456wert
S4200_C1	C	157	987123jkl456wert

Device	Cell	Channel	Wireless Passkey
S4200_C2	C	157	987123jkl456wert
S4200_C3	C	157	987123jkl456wert

3. In each cell, install the S4200 transmitters such that each one has a clear RF line of sight with its associated S4300 device.

This application can be illustrated this way, where the three cells are in the same location:



Installing more than three cells in the 2.4 GHz band or more than nine cells in the 5 GHz band requires more RF planning. In such a context, you should contact the customer service team for assistance.

## 5 GHz Band in Europe

The variety of supported colocalization setups is limited in Europe because of:

- DFS regulations, mainly with the automatic channel selection that forces the master devices to see each other.
- False radar detection that can happen when using adjacent channels. By default, only half the frequency channels are available, therefore ensuring that no adjacent channels are used; however, you can make all channels available (for more information, see page 33).

It is suggested to limit the number of colocated cells to six in the 5.40–5.725 GHz band. By respecting the following steps, you can assume that the cells will not share the same frequency channel, making the complete bandwidth available for each one:

1. Assign a different wireless passkey to each cell.

Ensure that all S4300 masters “see” one another. For the procedure, see Appendix D on page 158. This step is mandatory if automatic frequency channel selection is selected, and strongly suggested for manual selection.



2. Position the devices so that there is at least 3 feet (1 meter) between each antenna.
3. If automatic channel selection is used, set a different starting order in each master device: 1 for the first device, 2 for the device next to it, 3 for the third one, and so on.

Installing more than six cells in the 5.40–5.725 GHz band requires the use of adjacent channels. This situation demands greater distances between the antennas to reduce potential radio interference and false radar detection. Therefore, you should contact the customer service team for assistance.

### False Radar Detection

The design of wireless systems in a DFS context becomes difficult because not only can the master devices cause an interference, but the slaves on an adjacent channel can also generate interferences that can cause false radar detection. Therefore, to reduce the possibility of false radar detection, it is strongly suggested to:

- Limit the number of colocated cells to six.
- Decrease the tx power of the wireless links that have a good RF margin (15 dB or more). This way, the interference generated by the device is reduced.
- Separate as much as possible devices sharing the same pole or installed on the same roof.
- In a context of adjacent channels, ensure that the signal level of a potentially interfering device on the first adjacent channel does not exceed -50 dB, -36 dB on the second channel, and -32 dB on the third channel. For example, if you use channel 100, 104 is the first adjacent channel, 108 the second channel, and 112 the third channel.
- Manually select a frequency channel, to reduce the use of adjacent channels.

In addition, the following features help reduce the possibility of false detection events:

- Half channel selection—This feature eliminates the possibility of using adjacent channels. Enable this feature on all masters in a new installation to avoid the potential conflict of having two masters on adjacent channels; in the web interface, the parameter is called DFS/TPC Adjacent Channel Removal. By default this feature is enabled.

If this feature is enabled, the channel list becomes:

100(DFS), 108(DFS), 116(DFS), 124(DFS), 132(DFS), 140(DFS), 254(Auto DFS/TPC)

The full channel list is:

100(DFS), 104(DFS), 108(DFS), 112(DFS), 116(DFS), 120(DFS), 124(DFS), 128(DFS), 132(DFS), 136(DFS), 140(DFS), 254(Auto DFS/TPC)

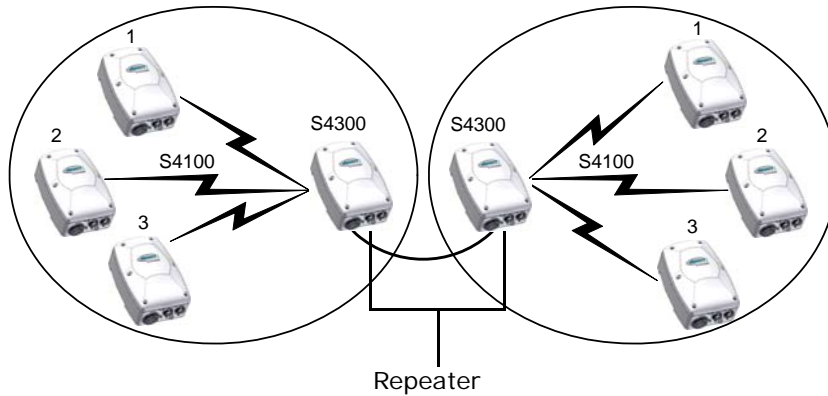
- Slave radar detection management—This feature allows you to disable radar detection on slave devices; in the web interface, the parameter is called Enable Radar Detection on Slave. In a typical DFS environment, the slave can detect a radar and alert its master to change the frequency channel. This situation can cause a major problem because it increases the number of nodes that can detect false radar events caused by adjacent channel interferences.

The default value is Disabled, meaning that the slave does not detect radars; in this case, the slave EIRP is reduced from 30 to 23 dBm and the Tx power is automatically reduced to meet the new maximum EIRP requirement.

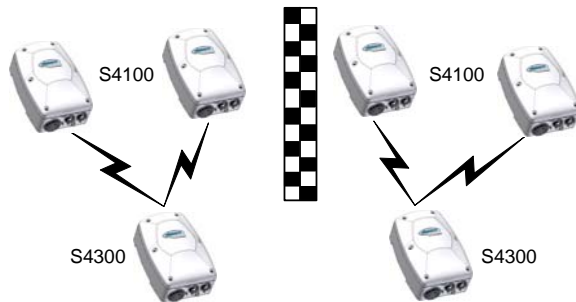
## Preferred Setups

In the 5.40–5.725 GHz band, the following colocated systems are the only ones supported when automatic frequency channel selection is enabled, since the master devices must see each other. In the manual channel selection mode, safe setups are:

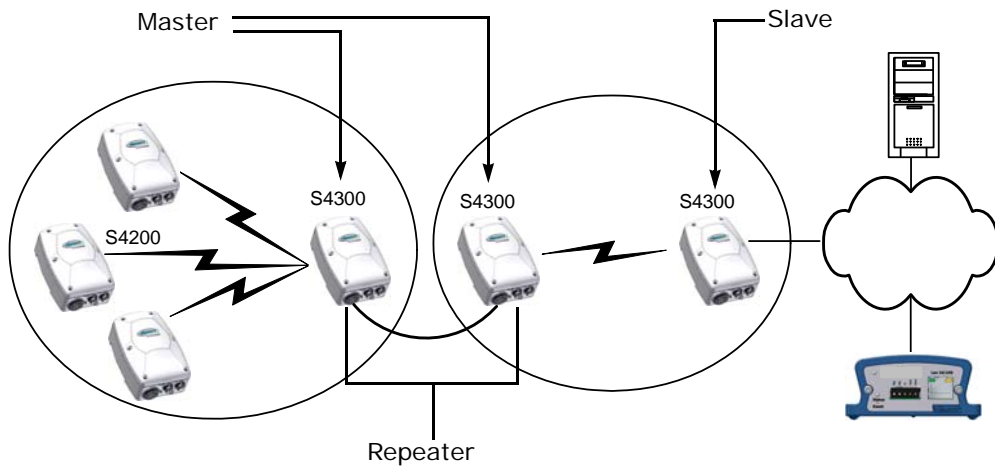
- A point-to-point repeater for one or more pairs of S4100 devices, with or without hidden nodes. Both master devices see each other.



- Two access point applications, in which the transmitters from one system do not see the transmitters from the other cell. Both master devices see each other.



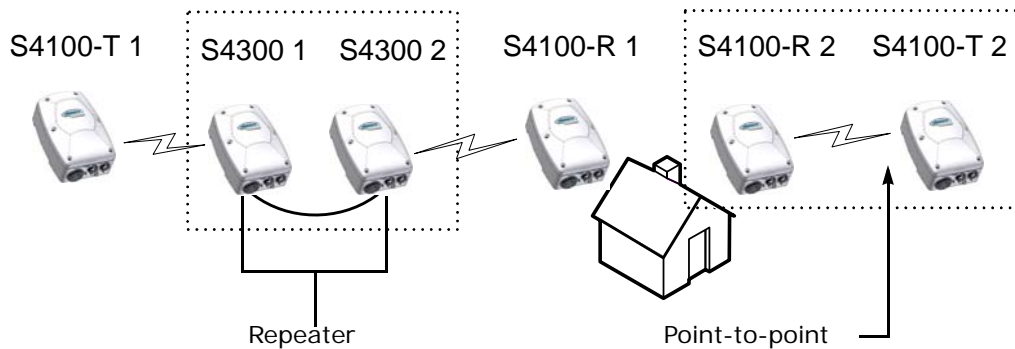
- A point-to-multipoint repeater. Both master devices see each other.



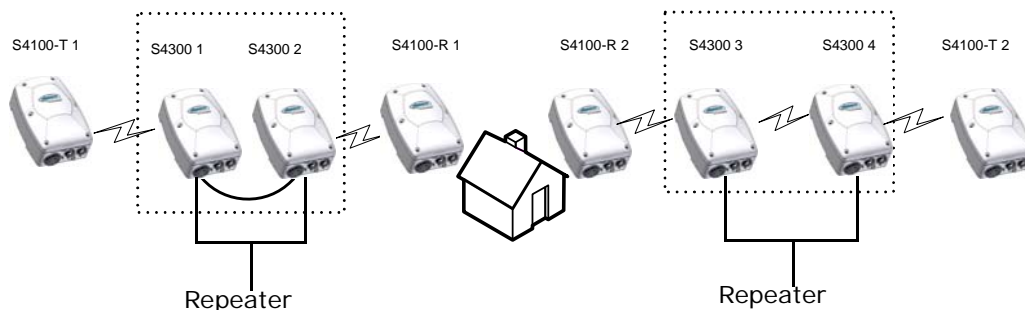
### Risky Setups

In the 5 GHz band in Europe, the following colocated systems are not supported if the automatic frequency channel selection is enabled, or are risky with manual selection mode if a radar is detected:

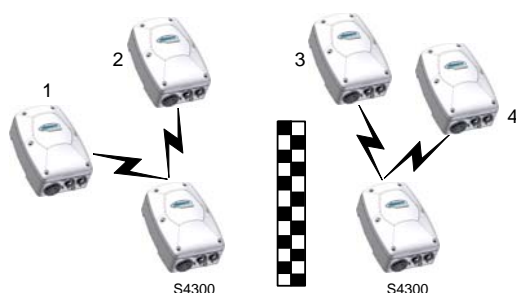
- A point-to-point repeater with a point-to-point link. In this setup, two masters do not see each other, S4300 2 and S4100-R 2, while the two receivers do.



- Multiple point-to-point repeaters. The S4300 2 and S4300 3 masters do not see each other, while the two receivers do.



- Access point applications with hidden masters. In this context, the two S4300 masters do not see each other, while transmitters 2 and 3 do.



## RF Planning

Successful operation of a wireless link depends on proper RF path planning and antenna installation. You have to install the devices in such a way that there is a clear RF line of sight between the two antennas. The factors to take into account are:

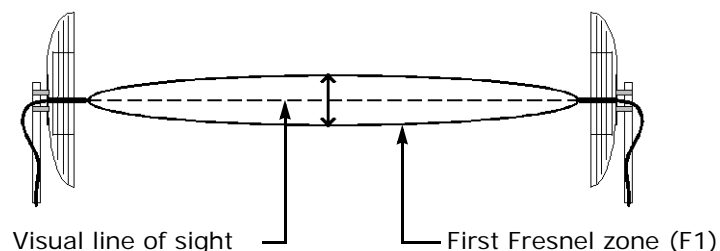
- Location evaluation
- Antenna requirements
- RF exposure

## Location Evaluation

The path between the two antennas must be free of obstacles that could disturb propagation. For very short link distances—less than 500 feet (152 meters)—you may be able to establish a working link despite partial path obstruction. However, radio waves will be in part absorbed and in part diffracted by the obstacles, therefore affecting link reliability. Because the reliability of such an installation is highly unpredictable, Verint does not recommend it. A path free of any obstacle is called an *RF line-of-sight path*.

To establish an RF line-of-sight path, you must take into account the spherical nature of the radio signal transmitted between the two antennas. This spherical signal spreads out from both ends of the communication path and creates a three dimensional elliptical area immediately surrounding the visual line of sight. This elliptical area varies in width depending on the length of the line of sight; the longer the length, the thicker the elliptical area becomes.

The region outlined by this elliptical area is known as the *first Fresnel zone*. The Fresnel zone is always thicker at the mid-point between the two antennas. Therefore what appears to be a perfect line-of-sight path between the base and a remote station may not be adequate for a radio signal; this is the difference between "visual" and "RF" line of sight.



In practice, it has been determined that a radio path can be considered an RF line-of-sight path if it has a clear opening through 60% of the first Fresnel zone (or  $0.6 F1$ ). Here are values for  $0.6 F1$  for various signal path distances and frequency bands:

Distance		Values for 60% of the First Fresnel Zone								Earth Curvature Effect	
		2.45 GHz		4.9 GHz		5.3 GHz		5.8 GHz			
mile	km	ft	m	ft	m	ft	m	ft	m	ft	m
1	1.6	14	4.2	9.8	3.0	9.5	2.9	8.9	2.7	0	0
4	6.5	27	8.4	19.5	5.9	18.7	5.7	18	5.5	2	0.6
7	11.3	37	11	25.8	7.9	25	7.6	23.6	7.2	6	1.8
15	24	53	16	37.8	11.5	36.4	11.1	35	10.6	29	8.8

For distances under 7 miles, the earth curvature effect is negligible. However, for greater distances, you need to consider it in your calculations; for instance, for a 15-mile link in the 2.4 GHz band, the two antennas must be located 82 feet higher than the highest obstacle in the RF line of sight between them (that is, 53 feet for the Fresnel zone plus 29 feet for the earth curvature effect). Consult the customer service team for assistance.

A common problem encountered in the field and related to the 0.6 F1 clearance rule is building obstruction. The proposed visual path may just barely clear a building but the RF line of sight will not. In such a case, the signal will be partially absorbed and diffracted. Increasing the height of the two antennas or the gain of the antennas are the only alternatives to improve the link quality.

**Note:** At 2.4, 4.9, and 5 GHz, radio waves are highly attenuated by dense foliage. A link established in the fall or winter season may be adversely affected in the spring and summertime, if it is established below tree level.

## Antenna Requirements

Verint offers many antennas to meet various distance requirements. You need to consider many factors when choosing an antenna, including the distance to cover, the RF bit rate, the radiated power (EIRP), and the frequency band. For systems located in North America on the 5 GHz band, you can use the *Wireless System Margin Calculator* located on the Verint Video Intelligence Solutions extranet (under Tools).

You must use only antennas certified by Verint. They meet the local regulations regarding the maximum antenna gain allowed. The certified antennas are listed in the “Compliance” appendix on page 183.

To ensure that the device meets the maximum EIRP in the region of operation, enter the antenna gain in the device (in the SConfigurator Wireless pane or the Wireless Communication page of the web interface); the device will automatically take it into account and adjust its own transmission power accordingly at startup.

For fixed point-to-point applications in the 5.725 GHz–5.850 GHz in USA and Canada, 19 dBi and 23 dBi antennas can be used without transmission power reduction. It is the responsibility of the installer to ensure that the system is used exclusively for fixed point-to-point operation.

**Note:** Connecting an antenna with a gain higher than the value for which the device is certified for the frequency band and region of operation is prohibited. It is your responsibility to ensure that you respect the regulations in place.

Antenna installation must be performed by certified professionals.

## RF Exposure Considerations

In order to comply with the RF exposure requirements of CFR 47 part 15 in North America, the devices must be installed in such a way as to allow a minimum separation distance of 12 inches (30 cm) between antennas and persons nearby.

Other countries may have different regulations. Please consult with local regulations prior to installation.

# 3

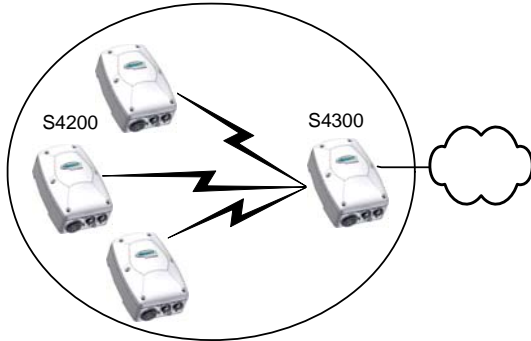
## Configuring and Installing an Access Point

The steps required to prepare your device for an access point operation are:

1. Configuring and installing the S4200 transmitters. For the procedure, refer to the *Nextiva S4200 Series User Guide*.
2. Assembling the power device.
3. Configuring the S4300.
4. Installing the S4300.
5. If required, installing an external antenna.

## Presenting the Application

A access point application is a wireless system made up of a master S4300 (the S4300 product code) and several S4200 slaves.



**Note:** Prior to deployment in the field, this wireless device requires configuration and testing.

## Connecting Power

On the S4300 model, you use the supplied power over Ethernet (PoE) kit to power the device and establish its Ethernet connection. You need to assemble the power device prior to installing it on the device. It is strongly recommended to execute this task in a lab.

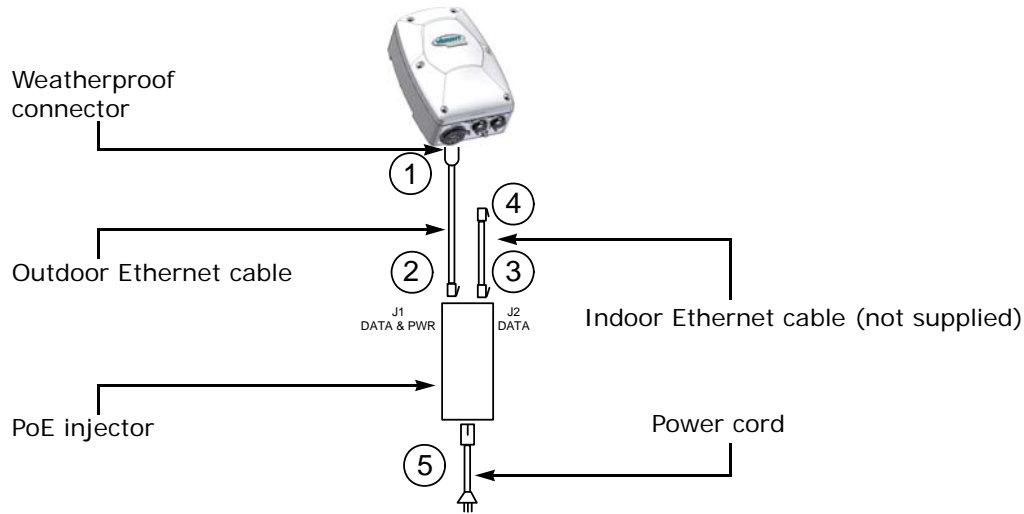
In addition to the kit, your shipment includes an Ethernet cable with a weatherproof connector at one end that will go directly on the device. The PoE kit sold by Verint contains two items: an injector and a power cord. The connection procedure may vary if you use another PoE kit; refer to the PoE kit documentation for more information.

**Note:** If you are not using the PoE kit supplied by Verint, ensure that the PoE injector used is UL listed and 802.3af compliant.

**Warning:** To avoid material damages, you must never power any two devices while their antennas are facing one another with a distance of less than 10 feet (3 meters).



#### To connect the PoE kit sold by Verint:



1. Plug the supplied outdoor Ethernet cable (the end with the weatherproof connector) into the network (RJ-45) connector of the S4300.
2. Plug the other end of the outdoor Ethernet cable into the DATA & PWR port of the injector.
3. Connect one end of the indoor Ethernet cable into the DATA port of the injector.
4. Connect the other end of the indoor Ethernet cable into an Ethernet equipment or your computer.

**Note:** The combined length of the two Ethernet cables cannot exceed 246 feet (75 meters). For example, if you used the supplied 82-foot (25m) cable in step 1, the maximum length of the indoor cable is 164 feet (50m).

**Warning:** To avoid damaging your equipment, ensure that your cable is connected into the DATA port of the PoE injector, and not in the DATA & PWR port.

5. Power the S4300 by plugging the power cord between the injector and the outlet.

## Configuring the System

Device configuration requires the use of the proprietary SConfigurator tool. Its latest version is included on the Verint web site ([www.verint.com/manuals](http://www.verint.com/manuals)). You need to copy its executable file (SConfigurator.exe) to the hard disk of your computer.

It is strongly recommended to configure the S4300 in a lab.

Configuring an S4300 device as an access point involves the following sequence of steps:

1. Setting the network parameters.

2. Setting the device name and country of operation.
3. Setting the wireless parameters.
4. Checking the communication between the devices.

For any other configuration task or for more information about the parameters, refer to the *Verint SConfigurator User Guide*.

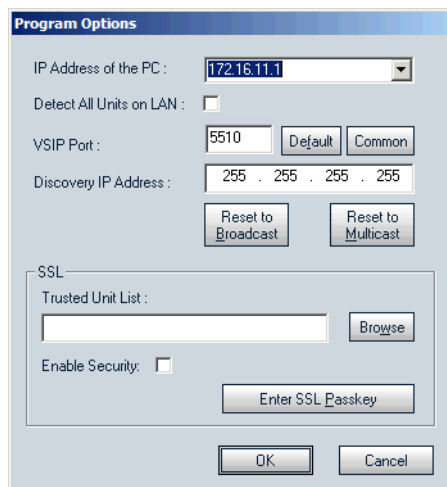
## Setting Network Parameters

The first step in configuring an S4300 device is to provide a typical initial configuration of its network parameters (including its IP address) to ensure compatibility with an existing network.

**Note:** To work properly, devices on the same network must have unique IP addresses. The device will not prevent you from entering a duplicate address. However, its system status LED will turn to flashing red (1-second interval); then the device will use its default address. You then need to configure it with a proper IP address.

### To set the initial network parameters:

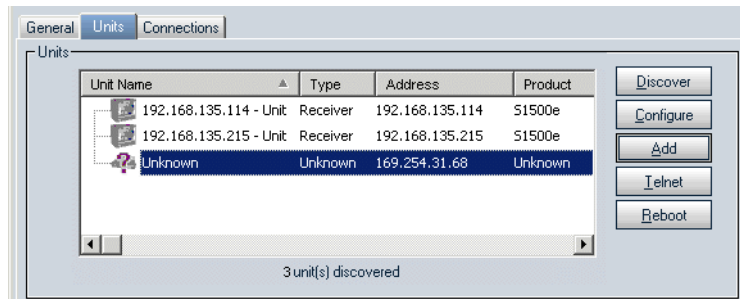
1. Ensure that the device is powered and connected to the Ethernet network.
2. Write down the serial number of the device in a safe place.
3. Start SConfigurator by double-clicking *SConfigurator.exe* on your hard disk. The SConfigurator window appears.
4. In the General tab, click **Program Options**. The Program Options window appears.



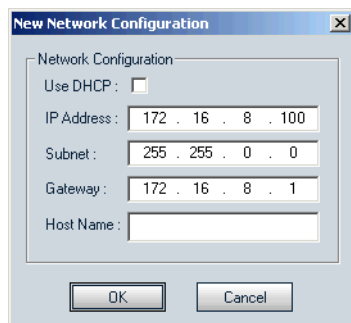
5. Check **Detect All Units on LAN**.
6. Ensure that the **VSIP Port** is 5510; otherwise, click **Default**.
7. Ensure that the **Discovery IP Address** is 255.255.255.255; otherwise, click **Reset to Broadcast**.

### 3: Configuring and Installing an Access Point

8. Click **OK**.
9. Select the **Units** tab, then click **Discover**. A device of type "Unknown" with a 169.254.X.Y IP address appears in the list; it corresponds to your new device. This default IP address is based on the APIPA (Automatic Private IP Addressing) addressing scheme. X and Y are relative to the MAC (Media Access Control) address of the device; for more information about APIPA, see page 152.



10. Select the unknown device, then click **Configure**.
11. In the Reconfigure unit? confirmation window, click **Yes**. The New Network Configuration window appears.



12. If you have a DHCP (Dynamic Host Configuration Protocol) server on your network, check **Use DHCP**. Otherwise, enter the IP address, subnet mask, and gateway of the device, as provided by your network administrator.

For more information about DHCP, see page 152.

13. Click **OK**.  
The device reboots with its new network configuration.
14. In the Units tab, click **Discover** to update the list of devices.  
The new S4300 device appears.
15. Select the device, then click **Configure**.  
The Unit Configuration window appears.

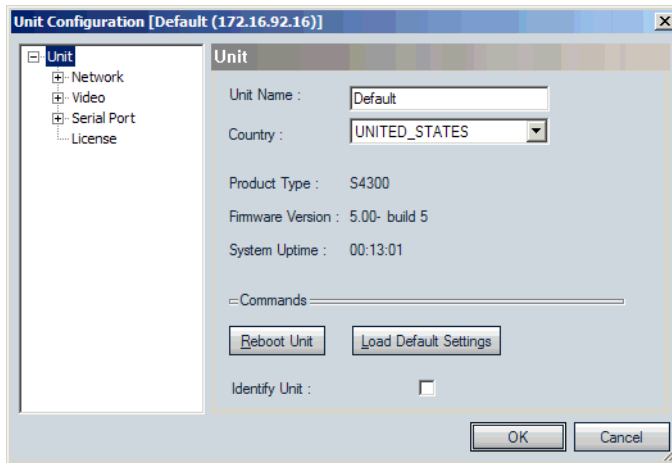
## Setting the Device Name and Country of Operation

It is recommended to give a meaningful name to each device, to help maintenance and debugging.

You must assign the proper country of operation to the device, so that it will comply to the DFS/TPC regulations, if applicable, respect the maximum EIRP, and use the proper set of frequency channels.

**To set the device name and country of operation:**

1. In the parameter tree of the Unit Configuration window, click **Unit**.



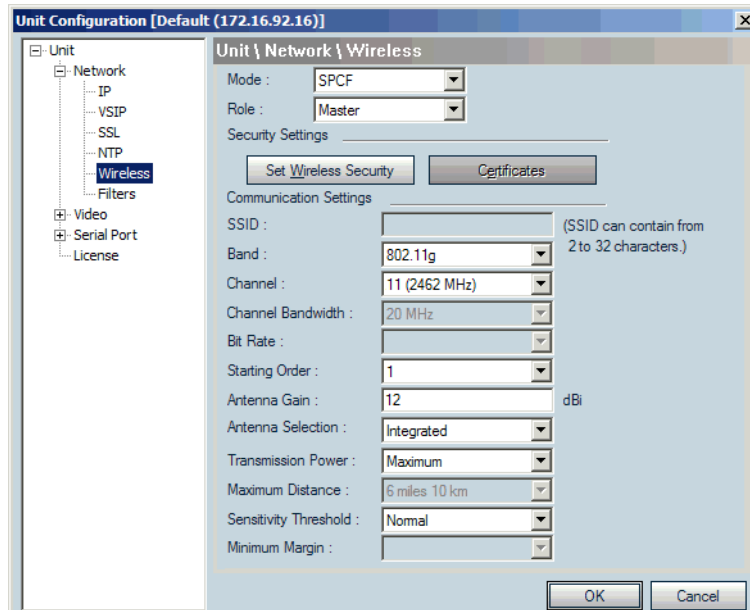
2. In the **Unit Name** box, assign a meaningful name to the device.
3. In the **Country** list, select the country of operation of the device.
4. In the confirmation window that appears, click **Yes**.

## Setting Wireless Parameters

The S4300 model is typically used as an access point. It can also be part of point-to-multipoint repeaters (for more information, see Chapter 6 on page 90).

#### To set the wireless parameters of an S4300 access point:

1. In the parameter tree of the Unit Configuration window, expand the **Network** structure, then click **Wireless**.



2. In the **Mode** list, select **SPCF**.
3. In the **Role** list, select **Master**.
4. In the **Band** list, select the frequency band that was used for the S4200 transmitters.
5. In the **Channel** list, select a frequency channel. You can select **Auto** for the automatic selection.

**Tip:** To simplify channel management, especially if your system involves colocated cells, you should manually assign a channel to the S4300, not use the automatic channel selection.

Once the devices are installed in their final location, you should perform a site survey to select the proper frequency channel. For the procedure, see page 149.

6. If necessary in the 4.9 GHz band, change the bandwidth in the **Channel Bandwidth** list.
7. In a DFS context with automatic channel selection and colocated wireless cells, enter in the **Starting Order** list a sequence number to delay its startup. This value must be different for each wireless cell. For more information about the starting order, see page 134.

8. If you are using an external antenna:
    - a. Enter its gain in the **Antenna Gain** box.
- Note: Providing a gain lower than the actual gain of the antenna you are using is prohibited.
- b. Select **External** in the **Antenna Selection** list.
  9. If you use the integrated antenna, check that the proper value is displayed in the **Antenna Gain** box; the gain is 8.5 dBi in the 2.4 GHz band and 12 dBi in the 4.9 GHz and 5 GHz bands.
  10. Set the wireless passkey to the same value as in the S4200 transmitters. For the procedure, see next.

#### To set the wireless passkey:

1. In the Wireless pane, click **Set Wireless Security**.

The Set Wireless Security window appears.

2. In the **Format** list, select the format of the passkey: **Text (ASCII)** or **Hexadecimal**.
3. In the **Passkey** box, enter the new passkey (case-sensitive).

The user-supplied passkey must be unique and have exactly 16 characters if the format is Text, or 32 digits if Hexadecimal. For the wireless connection to be secure, do not enter a known name (like a street name), but instead use a mix of digits and letters. Do not disclose the passkey. The connection security is based on the secrecy and uniqueness of the passkey.

4. In the **Confirmation** box, enter again the passkey.
5. To set the wireless passkey to its default value, click **Reset**.
6. On a master device, to apply the new password to all associated devices:
  - a. Ensure that **Apply changes to connected clients/slaves** is checked.
  - b. Click **OK**.

Note: The wireless passkey of the master will be changed only when you click OK in the Unit Configuration window.

The Changing Wireless Passkey window appears.

- c. When the procedure is finished, click **Close**.
7. In the Set Wireless Security window, click **OK**.
8. In the Unit Configuration window, click **OK**.
9. In the Warning! window that appears, click **Yes** to save the new parameters.
10. In the confirmation window that appears, click **OK**. The device reboots with its new wireless configuration.

## Checking Communication

Using SConfigurator, ensure that the master device and its slaves communicate well together.

### To check communication:

1. If required, power up all the devices making up the system.
2. In the Units tab in SConfigurator, ensure that the associated devices are hierarchically positioned under the master.
3. In the Network > Wireless > Link Status pane of the Unit Configuration window of the master, ensure that the associated devices are in the Clients/Slaves list.
4. Ensure that there is end-to-end video transmission in the lab before installing the devices in their final locations.

# Installing the System

After ensuring that all devices are communicating properly in a lab, you can install the S4300 access point in its final location. Depending on your setup, you can install an external antenna on the device.

**Note:** When installing colocated wireless systems, take into account the distance limitations listed on page 29.

## Mounting a Device on a Pole or Wall




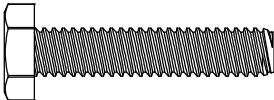
The S4300 model is a single device.

You can install an S4300 on a wall or pole using a mounting assembly set that is included in your shipment. The mounting assembly set includes:

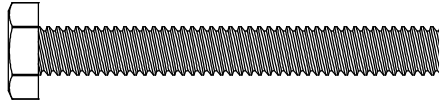
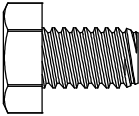
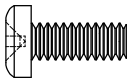
- A mounting bracket
- A pole/wall pivot mount
- A pole clamp
- Two stainless steel straps

**Note:** You must install the mounting assembly on the S4300. It is required to properly mount and securely ground the wireless device.

The following fasteners are also part of the set:

Item	Description	Scale Drawing
1	Lock washers for the pole clamp (2) and the pole/wall mount pivot (2)	
2	Lock washers for the mounting bracket (4)	
3	Nuts for the pole clamp (2) and the pole/wall mount pivot (2)	
4	Hex screws (7/16 inch) for the pole/wall mount pivot (2)	



Item	Description	Scale Drawing
5	Hex screws (7/16 inch) for the pole clamp (2)	 <p>Not a scale drawing. Real length is 3.5 inches (89 mm).</p>
6	Hex screw (0.5 inch) for the ground lug (1)	
7	Screws (Phillips) for the mounting bracket (4)	

To install the mounting assembly, you need the following equipment:

- Phillips #2 screwdriver
- Slotted screwdriver
- 0.5-inch (13-mm) wrench
- 7/16-inch (11-mm) wrench
- Four screws if the device is installed on a wall

The pole diameter can vary from 1.0 to 6.5 inches (2.55 to 16.5 cm).

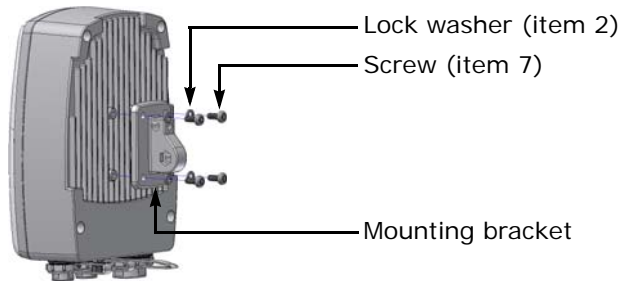
**Warning:** When installing colocated wireless systems, you have to take into account the distance limitations listed on page 29.

Always mount the device with the mating connectors pointing downwards.

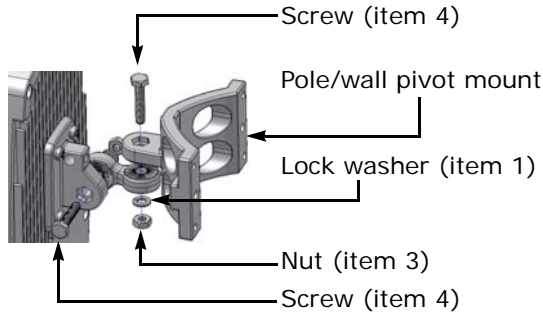
**Note:** If you are not installing a high-gain antenna, position the device so that its integrated antenna has a clear RF line of sight with the antennas of the facing devices.

**To mount an S4300 on a pole or wall:**

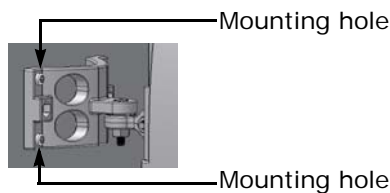
1. Install the mounting bracket on the rear of the device with a Phillips screwdriver, using the four screws (item 7) and the four lock washers (item 2). The recommended torque is 23 lbf-inch (2.6 N-m).



2. Attach the pole/wall pivot mount to the mounting bracket with a 7/16-inch (11-mm) wrench, using the two screws (item 4), two lock washers (item 1), and two nuts (item 3). The recommended torque is 70 lbf-inch (7.9 N-m).

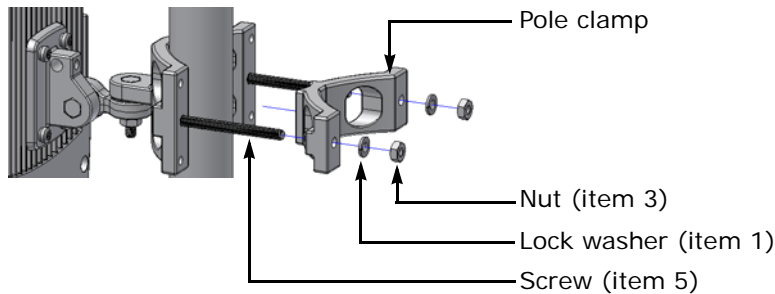


3. To install the device on a wall, use four screws (not supplied) in the four mounting holes located at the ends of the pole/wall pivot mount.

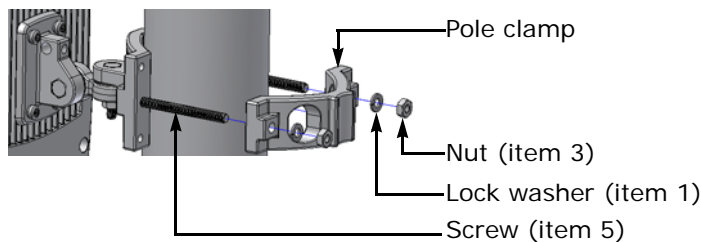


### 3: Configuring and Installing an Access Point

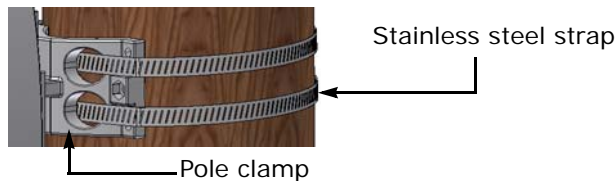
4. To install the device on a small pole (1–2.25 inch, or 2.55–5.7 cm diameter), position the device and the pole clamp the following way, then use a 7/16-inch (11-mm) wrench to put in place the two screws (item 5) with two nuts (item 3) and two lock washers (item 1). The recommended torque is 70 lbf-inch (7.9 N-m).



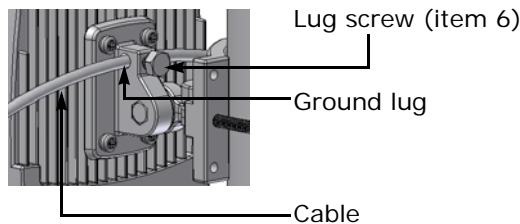
5. To install the device on a pole with a 2.25–3.25 inch diameter (5.7–8.25 cm), position the device and the pole clamp the following way, then use a 7/16-inch (11-mm) wrench to put in place the two screws (item 5) with two nuts (item 3) and two lock washers (item 1). The recommended torque is 70 lbf-inch (7.9 N-m).



6. To install the device on a pole with a 4.5–6.5 inch diameter (11.4–16.5 cm), use the supplied stainless steel straps and a slotted screwdriver.



7. Connect the device to the ground by inserting a copper cable into the ground lug, then screw in the lug screw (item 6) using a 0.5-inch (13-mm) wrench. Use a large diameter wire (minimum AWG 10; maximum AWG 1), and make it as short as possible. Then ground the cable.



8. If required, install an external antenna on the device (see next).

**Tip:** If you are installing the S4300 equipment in a lightning prone environment or in a site where large AC mains power fluctuations are a common occurrence, add external surge protection to secure your equipment. For more information, see Appendix C on page 154.

**Tip:** If the S4300 is directly exposed to the sun in an environment likely to reach 122°F (50°C), install a sun shield. Otherwise, reduce the maximum operating temperature by 18°F (10°C) to protect the equipment; that is, without a sun shield, the maximum temperature should be 104°F (40°C).

9. Connect the PoE kit to the device (see page 40).
10. Connect the loose end of the indoor Ethernet cable into an Ethernet equipment.

**Warning:** To avoid damaging your equipment, ensure that the Ethernet cable is connected into the DATA port of the PoE injector, and not in the DATA & PWR port.

11. Power the device by connecting the electric plug of the PoE injector into the outlet.
12. To improve the signal level between the devices, use the antenna alignment utility from SConfigurator.

## Installing an External Antenna

If you bought a high gain antenna, install it after the S4300 is in place.

**Note:** You can only use antennas certified by Verint. For the list, see the “Compliance” appendix on page 183.

The antenna requires professional installation.

The installer must enter the proper antenna gain in the device so that the transmission power is automatically adjusted. It is the responsibility of the installer to ensure that the proper antenna gain is configured. For fixed point-to-point applications in the 5.725 GHz–5.850 GHz in USA and Canada, 19 dBi and 23 dBi antennas can be used without transmission power reduction. It is the responsibility of the installer to ensure that the system is used exclusively for fixed point-to-point operation.

An omni-directional antenna (ANT-WP8-49/5x product code) is available for installation on a master device that requires a 360° coverage. Use it if the following conditions are met:

- There is a short distance between the master and slave devices (less than 0.6 mile/1 km). A typical use is in parking lots.
- At least three slaves are connected to the master.

- The antennas of the slaves point towards the omni-directional antenna and are in its vertical coverage zone (vertical beamwidth of 14°).
- The omni-directional antenna is installed vertically, without any tilt.

#### **To install an external antenna:**

1. Install the antenna above the S4300 device. If you bought your antenna from Verint, use the supplied pole mount bracket.
2. Remove the cap from the antenna connector on the S4300.
3. Screw the SMA connector of the antenna cable to the antenna connector on the S4300 and tighten it with a 0.25-inch (0.6 centimeter) wrench.

**Warning:** Do not over-tighten to avoid damaging the connector. The recommended torque is 8 lbf-inch (100 N-cm). You could use a calibrated SMA torque wrench (for instance, from the Pasternack company, available at [www.pasternack.com](http://www.pasternack.com)).

Never leave the antenna connector without either the cap or the SMA connector. The antenna connector must be terminated to avoid damaging the device radio.

4. Apply two or three layers of electrical tape around all RF connections.  
The antenna cable and connectors are weather-tight; however, vibration caused by the wind will over time loosen the connectors and reduce the efficiency of the gaskets. The electrical tape will prevent this situation.
5. With SConfigurator, enter the new antenna gain and change the antenna selection from Integrated to External.
6. Carefully align the antenna with those of the other devices so that they have a clear RF line of sight.
7. To improve the signal level between both devices, use the antenna alignment utility from SConfigurator.

# 4

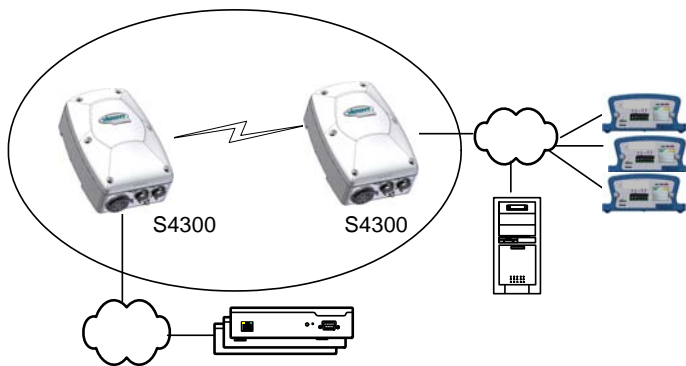
## Configuring and Installing a Wireless Bridge

The steps required to prepare your S4300-BR for wireless bridge operation are:

1. Assembling the power devices.
2. Configuring the two S4300 devices part of the wireless bridge (S4300-BR); always start with the master. You need to shut down the first device before configuring the second one.
3. Installing the S4300-BR.
4. If required, installing an external antenna.

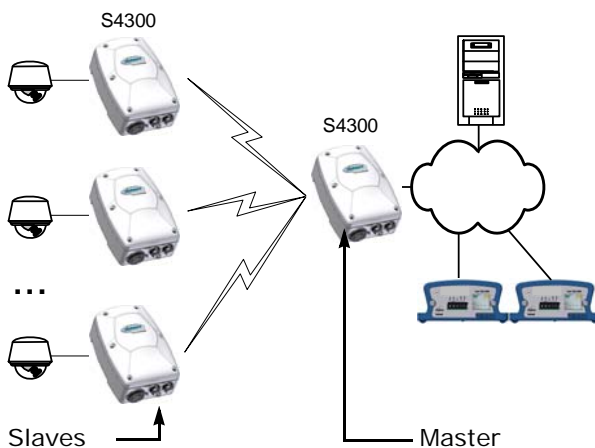
## Presenting the Application

The purpose of a wireless bridge is to access remote or hard-to-reach wired edge devices, or to send surveillance video data through a long distance link. You use the S4300-BR (made up of two devices, one master and one slave) to create this bridge. Any of the two devices can act as the master.



**Note:** Prior to deployment in the field, this wireless device requires configuration and testing.

You can also use the S4300-BR product in point-to-multipoint wireless bridges, to transmit video coming from IP cameras:



# Connecting Power

Depending on the device used, the power connection is different:

- The S4300-BR model uses either 12V DC or 24V AC.
- The S4300-BR-PoE model uses power over Ethernet (PoE).

You need to assemble the power devices prior to installing them on the devices. It is strongly recommended to execute these tasks in a lab.

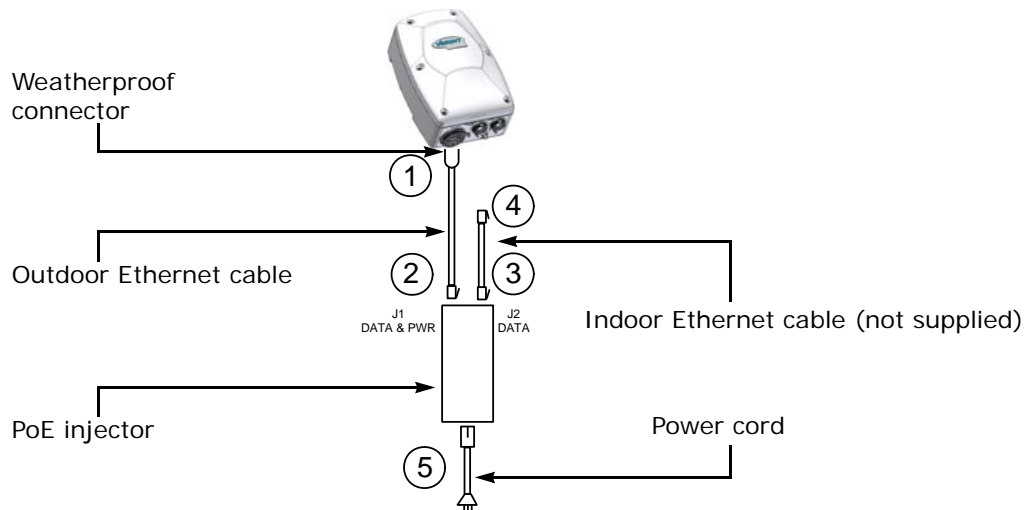
**Warning:** To avoid material damages, you must never power any two devices while their antennas are facing one another with a distance of less than 10 feet (3 meters).

## Power over Ethernet

On the S4300-BR-PoE model, you use the supplied PoE kits to power the devices and establish their Ethernet connection. In addition to the kits, your shipment includes two Ethernet cables with weatherproof connectors at one end that will go directly on the devices. The PoE kit sold by Verint contains two items: an injector and a power cord. The connection procedure may vary if you use another PoE kit; refer to the PoE kit documentation for more information.

**Note:** If you are not using the PoE kit supplied by Verint, ensure that the PoE injector used is UL listed and 802.3af compliant.

**To connect the PoE kit sold by Verint:**





#### 4: Configuring and Installing a Wireless Bridge

1. Plug the supplied outdoor Ethernet cable (the end with the weatherproof connector) into the network (RJ-45) connector of the S4300.
2. Plug the other end of the outdoor Ethernet cable into the DATA & PWR port of the injector.
3. Connect one end of the indoor Ethernet cable into the DATA port of the injector.
4. Connect the other end of the indoor Ethernet cable into an Ethernet equipment or your computer.

**Note:** The combined length of the two Ethernet cables cannot exceed 246 feet (75 meters). For example, if you used the supplied 82-foot (25m) cable in step 1, the maximum length of the indoor cable is 164 feet (50m).

**Warning:** To avoid damaging your equipment, ensure that your cable is connected into the DATA port of the PoE injector, and not in the DATA & PWR port.

5. Power the S4300 by plugging the power cord between the injector and the outlet.

## 12V DC/24V AC Power

Use the supplied power cable to power the devices.

**Note:** CE and FCC compliance testing has been performed with the MTA572415 (CE 24V AC) and MA572416 (24V AC North America) power supplies respectively. They correspond to the PS2440 power supply offered as an option by Verint.

Power supplies other than the approved ones require verification of operation with the S4300 before use.

If you are using a power supply other than the one supplied by Verint, you need to ensure that it has a minimum capacity of 1.6A (for 12V DC) or 25 VA (for 24V AC).

#### **To power the device:**

1. Plug the power cable on the main connector of the device.
2. In 12V DC, connect each power wire of the power cable to the corresponding wire of the power supply: the red wire to the input (+) wire and the black wire to the ground wire (-). For more information, refer to the power supply documentation.
3. In 24V AC, connect each power wire of the supplied cable to a wire on the power supply. Both wires are used for power.
4. Connect the electrical plug into the outlet.

# Configuring the System

Device configuration requires the use of the proprietary SConfigurator tool. Its latest version is included on the Verint web site ([www.verint.com/manuals](http://www.verint.com/manuals)). You need to copy its executable file (SConfigurator.exe) to the hard disk of your computer.

It is strongly recommended to configure the S4300-BR in a lab.

Configuring each device making up the S4300-BR product for a wireless bridge application involves the following sequence of steps:

**Note:** Never power more than one S4300 device at a time during the configuration process.

1. Setting the network parameters.
2. Setting the device name and country of operation.
3. Setting the wireless parameters.
4. Checking the communication between the devices.

For any other configuration task or for more information about the parameters, refer to the *Verint SConfigurator User Guide*.

## Setting Network Parameters

The first step in configuring an S4300 device is to provide a typical initial configuration of its network parameters (including its IP address) to ensure compatibility with an existing network.

**Note:** To work properly, devices on the same network must have unique IP addresses. The device will not prevent you from entering a duplicate address. However, its system status LED will turn to flashing red (1-second interval); then the device will use its default address. You then need to configure it with a proper IP address.

### To set the initial network parameters:

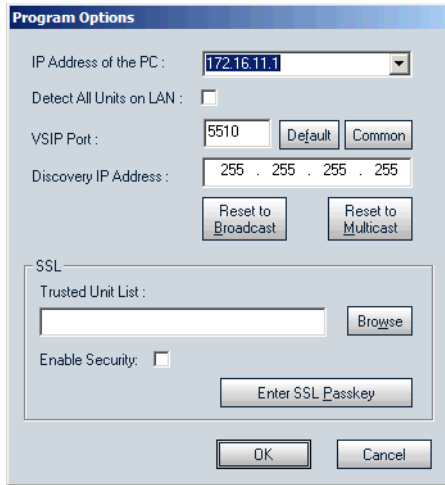
1. Ensure that the device is powered.
2. Write down the serial numbers of the devices in a safe place.
3. On a non-PoE device, plug an Ethernet cable between the network (RJ-45) connector on the device and the network or a computer.

**Note:** The maximum length of this Ethernet cable is 328 feet (100 meters).

4. Start SConfigurator by double-clicking SConfigurator.exe on your hard disk. The SConfigurator window appears.

#### 4: Configuring and Installing a Wireless Bridge

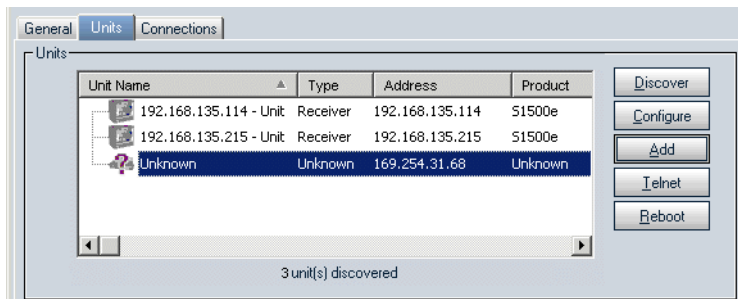
5. In the General tab, click **Program Options**. The Program Options window appears.



The Program Options dialog box contains the following fields and controls:

- IP Address of the PC: 172.16.11.1
- Detect All Units on LAN: ☐
- VSIP Port: 5510 (with Default and Common buttons)
- Discovery IP Address: 255 . 255 . 255 . 255 (with Reset to Broadcast and Reset to Multicast buttons)
- SSL section:
  - Trusted Unit List: (empty text box with Browse button)
  - Enable Security: ☐
  - Enter SSL Passkey: (text box)
- OK and Cancel buttons at the bottom.

6. Check **Detect All Units on LAN**.
7. Ensure that the **VSIP Port** is 5510; otherwise, click **Default**.
8. Ensure that the **Discovery IP Address** is 255.255.255.255; otherwise, click **Reset to Broadcast**.
9. Click **OK**.
10. Select the **Units** tab, then click **Discover**. A device of type "Unknown" with a 169.254.X.Y IP address appears in the list; it corresponds to your new device. This default IP address is based on the APIPA (Automatic Private IP Addressing) addressing scheme. X and Y are relative to the MAC (Media Access Control) address of the device; for more information about APIPA, see page 152.



The Units tab displays a table of discovered units:

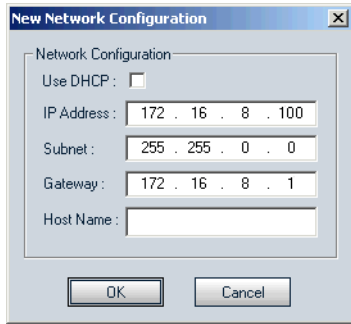
Unit Name	Type	Address	Product
192.168.135.114 - Unit	Receiver	192.168.135.114	S1500e
192.168.135.215 - Unit	Receiver	192.168.135.215	S1500e
Unknown	Unknown	169.254.31.68	Unknown

Buttons on the right: Discover, Configure, Add, Internet, Reboot.

3 unit(s) discovered

11. Select the unknown device, then click **Configure**.

12. In the Reconfigure unit? confirmation window, click **Yes**. The New Network Configuration window appears.



13. If you have a DHCP (Dynamic Host Configuration Protocol) server on your network, check **Use DHCP**. Otherwise, enter the IP address, subnet mask, and gateway of the device, as provided by your network administrator.

For more information about DHCP, see page 152.

14. Click **OK**.

The device reboots with its new network configuration.

15. In the Units tab, click **Discover** to update the list of devices.

The new S4300 device appears.

16. Select the device, then click **Configure**.

The Unit Configuration window appears.

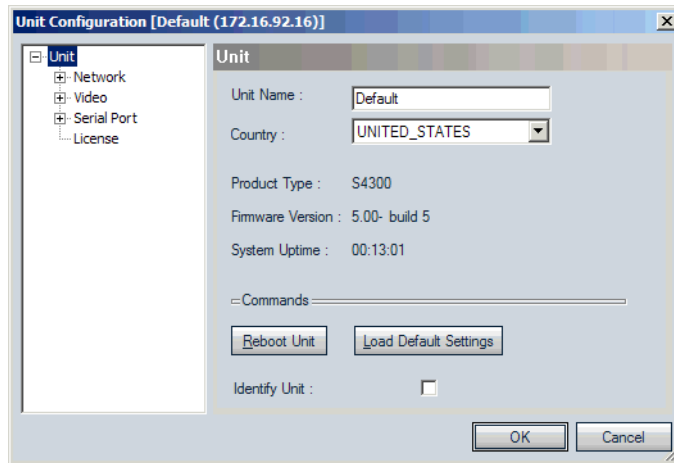
## Setting the Device Name and Country of Operation

It is recommended to give a meaningful name to each device, to help maintenance and debugging.

You must assign the proper country of operation to the device, so that it will comply to the DFS/TPC regulations, if applicable, respect the maximum EIRP, and use the proper set of frequency channels.

**To set the device name and country of operation:**

1. In the parameter tree of the Unit Configuration window, click **Unit**.



2. In the **Unit Name** box, assign a meaningful name to the device.
3. In the **Country** list, select the country of operation of the device.
4. In the confirmation window that appears, click **Yes**.

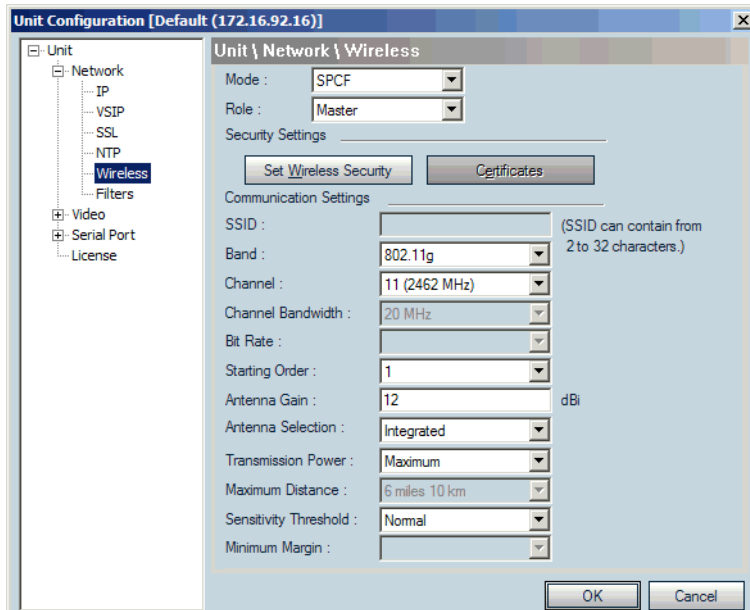
## Setting Wireless Parameters

The set of wireless parameters to apply vary depending if the device:

- is a master or a slave in a wireless bridge.
- is part of a point-to-multipoint bridge. For the description, see page 55.
- is part of a wireless bridge repeater. For the values to apply, see page 114.

**To set the wireless parameters of a master device:**

1. In the parameter tree of the Unit Configuration window, expand the **Network** structure, then click **Wireless**.



2. In the **Mode** list, select **SPCF**.
3. In the **Role** list, select **Master**.
4. In the **Band** list, select a frequency band.
5. In the **Channel** list, select a frequency channel. You can select **Auto** for the automatic selection.

**Tip:** To simplify channel management, especially if your system involves colocated cells, you should manually assign a channel to the S4300, not use the automatic channel selection.

Once the devices are installed in their final location, you should perform a site survey to select the proper frequency channel. For the procedure, see page 149.

6. If necessary in the 4.9 GHz band, change the bandwidth in the **Channel Bandwidth** list.
7. In a DFS context with automatic channel selection and colocated wireless cells, enter in the **Starting Order** list a sequence number to delay its startup. This value must be different for each wireless cell. For more information about the starting order, see page 134.

8. If you are using an external antenna:
  - a. Enter its gain in the **Antenna Gain** box.

Note: Providing a gain lower than the actual gain of the antenna you are using is prohibited.

- b. Select **External** in the **Antenna Selection** list.
9. If you use the integrated antenna, check that the proper value is displayed in the **Antenna Gain** box; the gain is 8.5 dBi in the 2.4 GHz band and 12 dBi in the 4.9 GHz and 5 GHz bands.
10. Set the wireless passkey to the value common to all devices in the cell. For the procedure, see page 64.

##### To set the wireless parameters of a slave device:

1. In the parameter tree of the Unit Configuration window, expand the **Network** structure, then click **Wireless**.
2. In the Mode list, select **SPCF**.
3. In the Role field, select **Slave**.
4. In the **Band** list, select the same frequency band as in the master.
5. If necessary in the 4.9 GHz band, change the bandwidth in the **Channel Bandwidth** list.
6. In the **Bit Rate** list, select the data rate at which the devices will operate in the wireless cell.
7. If you are using an external antenna:
  - a. Enter its gain in the **Antenna Gain** box.

Note: Providing a gain lower than the actual gain of the antenna you are using is prohibited.

- b. Select **External** in the **Antenna Selection** list.
8. If you use the integrated antenna, check that the proper value is displayed in the **Antenna Gain** box; the gain is 8.5 dBi in the 2.4 GHz band and 12 dBi in the 4.9 GHz and 5 GHz bands.
9. Set the wireless passkey to the value common to all devices in the cell. For the procedure, see page 64.

## To set the wireless passkey:

1. In the Wireless pane, click **Set Wireless Security**.

The Set Wireless Security window appears.

2. In the **Format** list, select the format of the passkey: **Text (ASCII)** or **Hexadecimal**.
3. In the **Passkey** box, enter the new passkey (case-sensitive).

The user-supplied passkey must be unique and have exactly 16 characters if the format is Text, or 32 digits if Hexadecimal. For the wireless connection to be secure, do not enter a known name (like a street name), but instead use a mix of digits and letters. Do not disclose the passkey. The connection security is based on the secrecy and uniqueness of the passkey.

4. In the **Confirmation** box, enter again the passkey.
5. To set the wireless passkey to its default value, click **Reset**.
6. On a master device, to apply the new password to all associated devices:
  - a. Ensure that **Apply changes to connected clients/slaves** is checked.
  - b. Click **OK**.

**Note:** The wireless passkey of the master will be changed only when you click OK in the Unit Configuration window.

The Changing Wireless Passkey window appears.

- c. When the procedure is finished, click **Close**.
7. In the Set Wireless Security window, click **OK**.



8. In the Unit Configuration window, click **OK**.
9. In the Warning! window that appears, click **Yes** to save the new parameters.
10. In the confirmation window that appears, click **OK**.

The device reboots with its new wireless configuration.

## Checking Communication

Using SConfigurator, ensure that the master device and its slaves communicate well together.

### To check communication:

1. If required, power up all the devices making up the system.
2. In the Units tab in SConfigurator, ensure that the associated devices are hierarchically positioned under the master.
3. In the Network > Wireless > Link Status pane of the Unit Configuration window of the master, ensure that the associated devices are in the Clients/Slaves list.
4. Ensure that there is end-to-end video transmission in the lab before installing the devices in their final locations.

## Installing the System

After ensuring that all devices are communicating properly in a lab, you can install the S4300 devices in their final location. Depending on your setup, you can install external antennas on the devices.

**Note:** When installing colocated wireless systems, take into account the distance limitations listed on page 29.

## Mounting a Device on a Pole or Wall




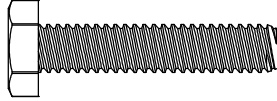
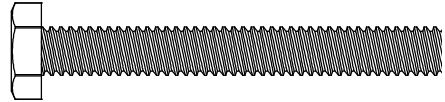
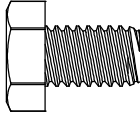
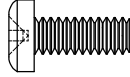
A wireless bridge is made up of two devices, each connected to a network or an IP camera with an Ethernet cable.

You can install an S4300 on a wall or pole using a mounting assembly set that is included in your shipment. The mounting assembly set includes:

- A mounting bracket
- A pole/wall pivot mount
- A pole clamp
- Two stainless steel straps

**Note:** You must install the mounting assembly on the S4300. It is required to properly mount and securely ground the wireless device.

The following fasteners are also part of the set:

Item	Description	Scale Drawing
1	Lock washers for the pole clamp (2) and the pole/wall mount pivot (2)	
2	Lock washers for the mounting bracket (4)	
3	Nuts for the pole clamp (2) and the pole/wall mount pivot (2)	
4	Hex screws (7/16 inch) for the pole/wall mount pivot (2)	
5	Hex screws (7/16 inch) for the pole clamp (2)	 Not a scale drawing. Real length is 3.5 inches (89 mm).
6	Hex screw (0.5 inch) for the ground lug (1)	
7	Screws (Phillips) for the mounting bracket (4)	

To install the mounting assembly, you need the following equipment:

- Phillips #2 screwdriver
- Slotted screwdriver
- 0.5-inch (13-mm) wrench
- 7/16-inch (11-mm) wrench
- Four screws if the device is installed on a wall

#### 4: Configuring and Installing a Wireless Bridge

The pole diameter can vary from 1.0 to 6.5 inches (2.55 to 16.5 cm).

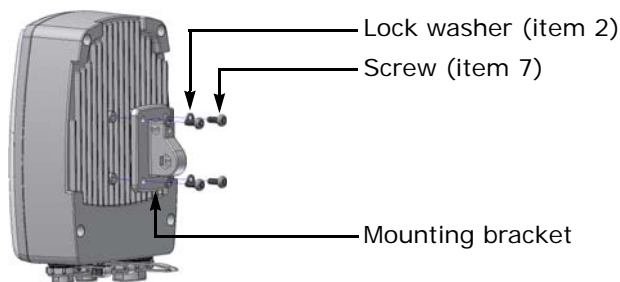
**Warning:** When installing colocated wireless systems, you have to take into account the distance limitations listed on page 29.

Always mount the device with the mating connectors pointing downwards.

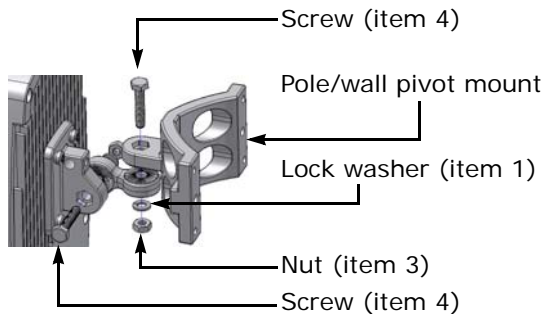
**Note:** If you are not installing a high-gain antenna, position the device so that its integrated antenna has a clear RF line of sight with the antennas of the facing devices.

##### To mount an S4300 on a pole or wall:

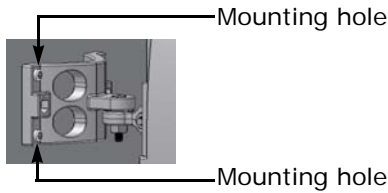
1. Install the mounting bracket on the rear of the device with a Phillips screwdriver, using the four screws (item 7) and the four lock washers (item 2). The recommended torque is 23 lbf-inch (2.6 N-m).



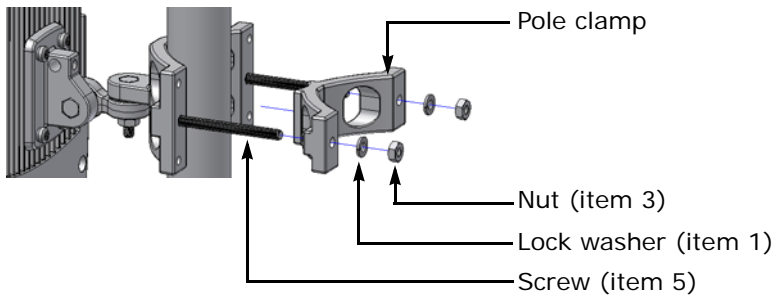
2. Attach the pole/wall pivot mount to the mounting bracket with a 7/16-inch (11-mm) wrench, using the two screws (item 4), two lock washers (item 1), and two nuts (item 3). The recommended torque is 70 lbf-inch (7.9 N-m).



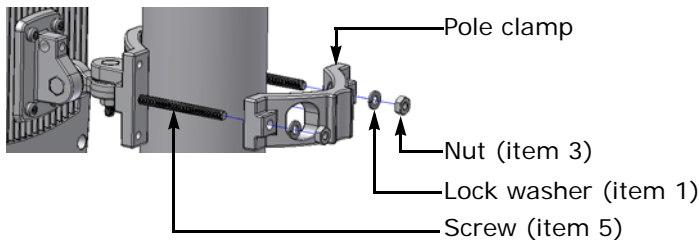
3. To install the device on a wall, use four screws (not supplied) in the four mounting holes located at the ends of the pole/wall pivot mount.



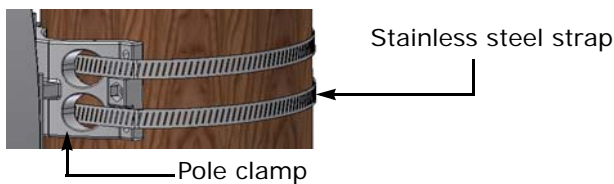
4. To install the device on a small pole (1–2.25 inch, or 2.55–5.7 cm diameter), position the device and the pole clamp the following way, then use a 7/16-inch (11-mm) wrench to put in place the two screws (item 5) with two nuts (item 3) and two lock washers (item 1). The recommended torque is 70 lbf-inch (7.9 N-m).



5. To install the device on a pole with a 2.25–3.25 inch diameter (5.7–8.25 cm), position the device and the pole clamp the following way, then use a 7/16-inch (11-mm) wrench to put in place the two screws (item 5) with two nuts (item 3) and two lock washers (item 1). The recommended torque is 70 lbf-inch (7.9 N-m).

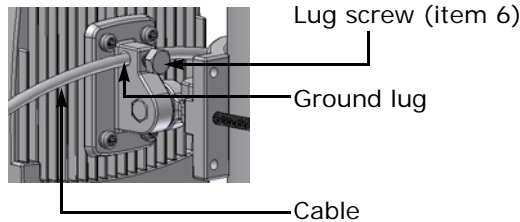


6. To install the device on a pole with a 4.5–6.5 inch diameter (11.4–16.5 cm), use the supplied stainless steel straps and a slotted screwdriver.



#### 4: Configuring and Installing a Wireless Bridge

7. Connect the device to the ground by inserting a copper cable into the ground lug, then screw in the lug screw (item 6) using a 0.5-inch (13-mm) wrench. Use a large diameter wire (minimum AWG 10; maximum AWG 1), and make it as short as possible. Then ground the cable.



8. If required, install an external antenna on the device (see page 70).

**Tip:** If you are installing the S4300 equipment in a lightning prone environment or in a site where large AC mains power fluctuations are a common occurrence, add external surge protection to secure your equipment. For more information, see Appendix C on page 154.

**Tip:** If the S4300 is directly exposed to the sun in an environment likely to reach 122°F (50°C), install a sun shield. Otherwise, reduce the maximum operating temperature by 18°F (10°C) to protect the equipment; that is, without a sun shield, the maximum temperature should be 104°F (40°C).

9. On the S4300-BR-PoE:
  - a. Connect the PoE kit to the device (see page 56).
  - b. Connect the loose end of the indoor Ethernet cable into an Ethernet equipment.

**Warning:** To avoid damaging your equipment, ensure that the Ethernet cable is connected into the DATA port of the PoE injector, and not in the DATA & PWR port.

- c. Power the device by connecting the electric plug of the PoE injector into the outlet.

10. On the S4300-BR:

- a. To properly fuse the power supplied to the wireless device, install a fuse between the power source and the power cable. The fuse must have the following ratings: UL Listed, 250V, 2.5A, Fast-Acting.

- b. Power the device using the assembled power device.

**Note:** Power supplies other than the approved ones (PS2440) require verification of operation with the S4300-BR before use.

If you are using a power supply other than the one supplied by Verint, you need to ensure that it has a minimum capacity of 1.6A (for 12V DC) or 25 VA (for 24V AC).

- c. Connect the device to the network or an Ethernet equipment using the supplied outdoor Ethernet cable.

11. Repeat step 1 to step 10 for the other device.

12. To improve the signal level between the devices, use the antenna alignment utility from SConfigurator.

## Installing an External Antenna

If you bought a high gain antenna, install it after the S4300 is in place.

**Note:** You can only use antennas certified by Verint. For the list, see the “Compliance” appendix on page 183.

The antenna requires professional installation.

The installer must enter the proper antenna gain in the device so that the transmission power is automatically adjusted. It is the responsibility of the installer to ensure that the proper antenna gain is configured. For fixed point-to-point applications in the 5.725 GHz–5.850 GHz in USA and Canada, 19 dBi and 23 dBi antennas can be used without transmission power reduction. It is the responsibility of the installer to ensure that the system is used exclusively for fixed point-to-point operation.

An omni-directional antenna (ANT-WP8-49/5x product code) is available for installation on a master device that requires a 360° coverage. Use it if the following conditions are met:

- There is a short distance between the master and slave devices (less than 0.6 mile/1 km). A typical use is in parking lots.
- At least three slaves are connected to the master.
- The antennas of the slaves point towards the omni-directional antenna and are in its vertical coverage zone (vertical beamwidth of 14°).
- The omni-directional antenna is installed vertically, without any tilt.

### To install an external antenna:

1. Install the antenna above the S4300 device. If you bought your antenna from Verint, use the supplied pole mount bracket.
2. Remove the cap from the antenna connector on the S4300.

3. Screw the SMA connector of the antenna cable to the antenna connector on the S4300 and tighten it with a 0.25-inch (0.6 centimeter) wrench.

**Warning:** Do not over-tighten to avoid damaging the connector. The recommended torque is 8 lbf-inch (100 N-cm). You could use a calibrated SMA torque wrench (for instance, from the Pasternack company, available at [www.pasternack.com](http://www.pasternack.com)).

Never leave the antenna connector without either the cap or the SMA connector. The antenna connector must be terminated to avoid damaging the device radio.

4. Apply two or three layers of electrical tape around all RF connections.

The antenna cable and connectors are weather-tight; however, vibration caused by the wind will over time loosen the connectors and reduce the efficiency of the gaskets. The electrical tape will prevent this situation.

5. With SConfigurator, enter the new antenna gain and change the antenna selection from Integrated to External.
6. Carefully align the antenna with those of the other devices so that they have a clear RF line of sight.
7. To improve the signal level between both devices, use the antenna alignment utility from SConfigurator.

# 5

## Configuring and Installing a Point-to-Point Repeater

The steps required to prepare your devices for point-to-point repeater operation are:

1. Configuring and installing the S4100 pairs in repeater mode. For the procedure, refer to the *Nextiva S4100 Series User Guide*.

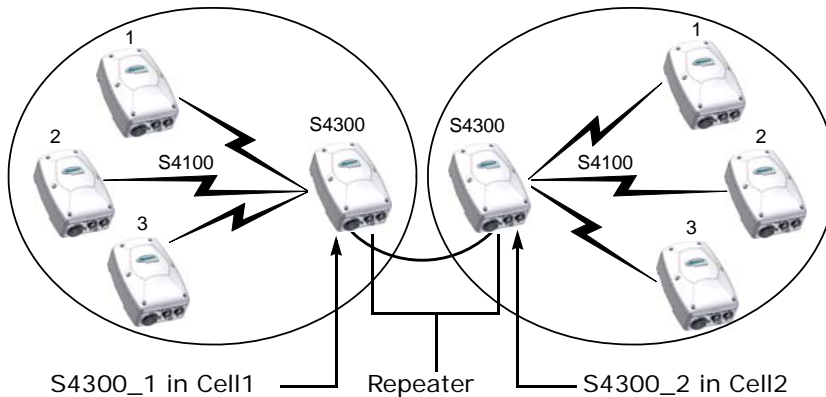
Note: You must complete the configuration of the S4100 devices before powering up an S4300.

2. Assembling the power devices.
3. Configuring the two S4300 devices part of the repeater (S4300-RP), one at a time. You need to shut down the first device before configuring the second one.
4. Installing the S4300-RP.
5. If required, installing an external antenna.



## Presenting the Application

A point-to-point repeater is a range extender for wireless links to retransmit the signals coming from one or many S4100 transmitters to their corresponding receivers. You use the S4300-RP (made up of two S4300 devices) to create this repeater.



Note: Prior to deployment in the field, this wireless device requires configuration and testing.

## Connecting Power

The S4300-RP uses 12V DC or 24V AC for power. It is strongly recommended to connect power in a lab.

Warning: To avoid material damages, you must never power any two devices while their antennas are facing one another with a distance of less than 10 feet (3 meters).

Use the supplied power cable to power the devices.

Note: CE and FCC compliance testing has been performed with the MTA572415 (CE 24V AC) and MA572416 (24V AC North America) power supplies respectively. They correspond to the PS2440 power supply offered as an option by Verint.

Power supplies other than the approved ones require verification of operation with the S4300 before use.

If you are using a power supply other than the one supplied by Verint, you need to ensure that it has a minimum capacity of 1.6A (for 12V DC) or 25 VA (for 24V AC).

### To power the device:

1. Plug the power cable on the main connector of the device.

2. In 12V DC, connect each power wire of the power cable to the corresponding wire of the power supply: the red wire to the input (+) wire and the black wire to the ground wire (-). For more information, refer to the power supply documentation.
3. In 24V AC, connect each power wire of the supplied cable to a wire on the power supply. Both wires are used for power.
4. Connect the electrical plug into the outlet.

## Configuring the System

Device configuration requires the use of the proprietary SConfigurator tool. Its latest version is included on the Verint web site ([www.verint.com/manuals](http://www.verint.com/manuals)). You need to copy its executable file (SConfigurator.exe) to the hard disk of your computer.

It is strongly recommended to configure the S4300-RP in a lab.

Configuring each device making up the S4300-RP product for a point-to-point repeater involves the following sequence of steps:

**Note:** Never power more than one S4300 device at a time during the configuration process.

1. Changing the IP address of the computer running SConfigurator.
2. Setting the network parameters.
3. Setting the device name and country of operation.
4. Setting the wireless parameters.
5. Checking the communication between the devices.
6. Putting back the original IP address of the computer.

For any other configuration task or for more information about the parameters, refer to the *Verint SConfigurator User Guide*.

## Changing the IP Address of the Computer

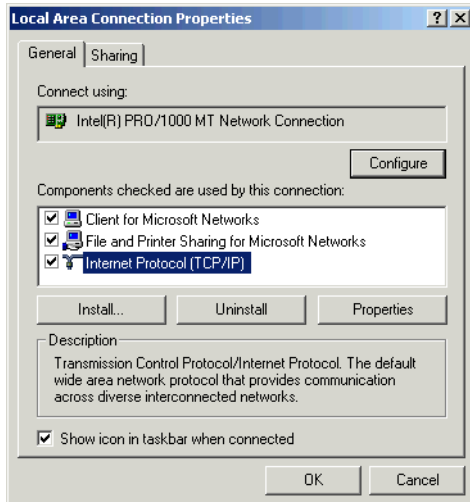
To change the parameters of the S4300 devices in a point-to-point repeater context, you need to temporarily change the IP address of your computer. The temporary address must be in the 172.16.23.255 subnet. The procedure varies depending on your operating system (Windows 2000 or Windows XP).

The recommended temporary IP settings are:

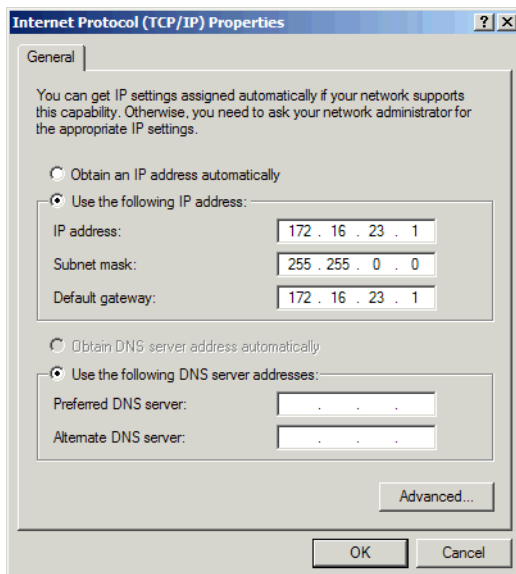
- IP address: 172.16.23.1
- Subnet mask: 255.255.0.0
- Default gateway: 172.16.23.1

### To change the IP address under Windows 2000:

1. From the desktop, right-click **My Network Places**, then choose **Properties**. The Network and Dial-up Connections window appears.
2. Double-click **Local Area Connection**. The Local Area Connection Status window appears.
3. Click **Properties**. The Local Area Connection Properties window appears.



4. In the component list, select **Internet Protocol (TCP/IP)**, then click **Properties**. The Internet Protocol (TCP/IP) Properties window appears.



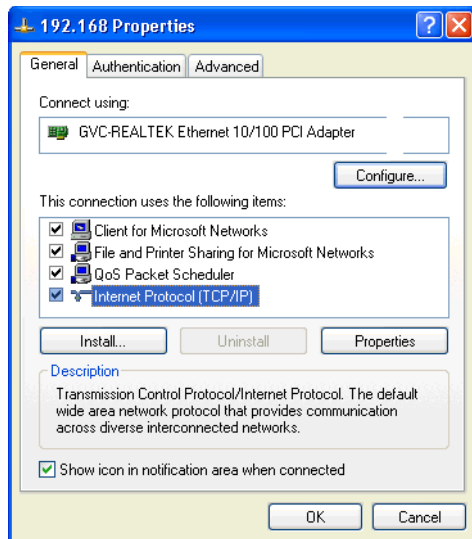
5. If **Use the following IP address** is selected, write down the information displayed in the box: the IP address, subnet mask, and default gateway.

You will need these addresses to put back your computer in its initial state once the configuration process is completed.

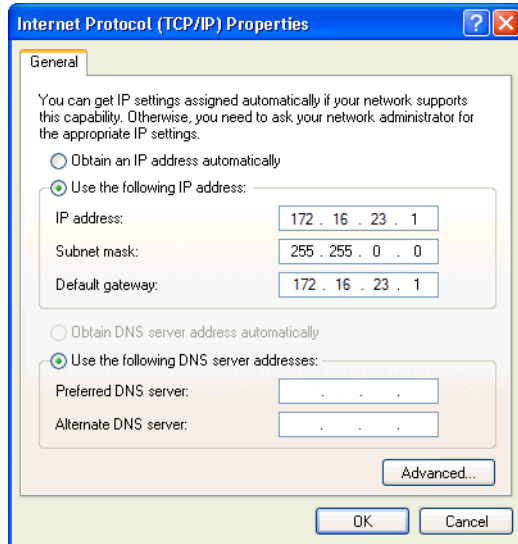
6. If **Obtain an IP address automatically** is selected, click **Use the following IP address**.
7. Enter the desired IP address, subnet mask, and default gateway (the temporary values when you are starting the configuration procedure, or the initial values when the work is over).
8. Click **OK** to close all windows.

#### To change the IP address under Windows XP:

1. In the Windows Start menu, select **Control Panel**.
2. If the classic view is enabled, select **Network Selection**. In the category view, select **Network and Internet Connections**, then **Network Connections**.
3. Double-click your active LAN or Internet connection.
4. Click **Properties**. A Properties window appears.



5. In the General tab, select the **Internet Protocol (TCP/IP)** item, then click **Properties**. The Internet Protocol (TCP/IP) Properties window appears.



6. If **Use the following IP address** is selected, write down the information displayed in the box: the IP address, subnet mask, and default gateway.

You will need these addresses to put back your computer in its initial state once the configuration process is completed.

7. If **Obtain an IP address automatically** is selected, click **Use the following IP address**.
8. Enter the desired IP address, subnet mask, and default gateway (the temporary values when you are starting the configuration procedure, or the initial values when the work is over).
9. Click **OK** to close all windows.

## Setting Network Parameters

The first step in configuring an S4300 device is to provide a typical initial configuration of its network parameters (including its IP address) to ensure compatibility with an existing network.

**Note:** To work properly, devices on the same network must have unique IP addresses. The device will not prevent you from entering a duplicate address. However, its system status LED will turn to flashing red (1-second interval); then the device will use its default address. You then need to configure it with a proper IP address.

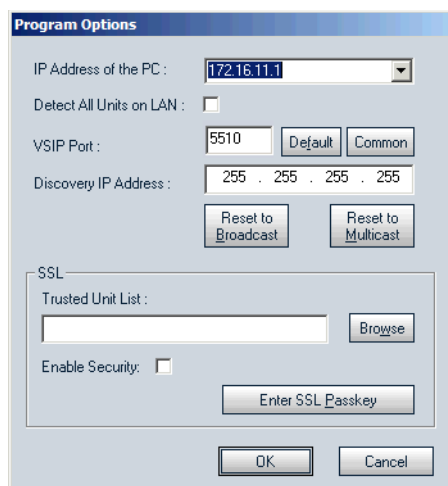
### To set the initial network parameters:

1. Ensure that the device is powered.
2. Write down the serial numbers of the devices in a safe place.

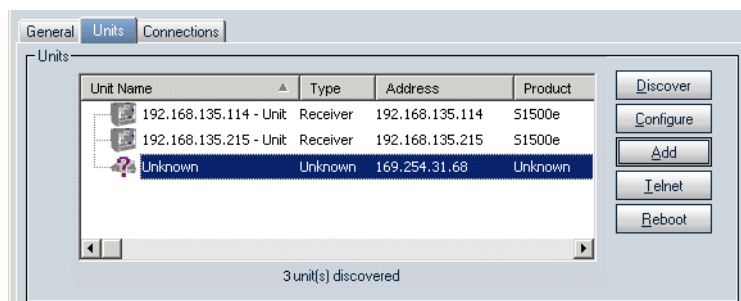
3. Plug an Ethernet cable between the network (RJ-45) connector on the device and the network or a computer.

Note: The maximum length of this Ethernet cable is 328 feet (100 meters).

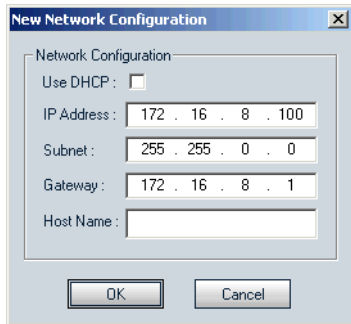
4. Start SConfigurator by double-clicking SConfigurator.exe on your hard disk. The SConfigurator window appears.
5. In the General tab, click **Program Options**. The Program Options window appears.



6. Check **Detect All Units on LAN**.
7. Ensure that the **VSIP Port** is 5510; otherwise, click **Default**.
8. Ensure that the **Discovery IP Address** is 255.255.255.255; otherwise, click **Reset to Broadcast**.
9. Click **OK**.
10. Select the **Units** tab, then click **Discover**. A device of type "Unknown" with a 169.254.X.Y IP address appears in the list; it corresponds to your new device. This default IP address is based on the APIPA (Automatic Private IP Addressing) addressing scheme. X and Y are relative to the MAC (Media Access Control) address of the device; for more information about APIPA, see page 152.



11. Select the unknown device, then click **Configure**.
12. In the Reconfigure unit? confirmation window, click **Yes**. The New Network Configuration window appears.



13. Do not check the **Use DHCP** box.
14. In the **IP Address** box, enter 172.16.23.51 for the S4300 on the transmitter side and 172.16.23.52 for the S4300 on the receiver side.
15. In the **Subnet** box, enter 255.255.0.0.
16. In the **Gateway** box, enter 172.16.23.1.
17. Click **OK**.

The device reboots with its new network configuration.

18. In the Units tab, click **Discover** to update the list of devices.

The new S4300 device appears.

19. Select the device, then click **Configure**.

The Unit Configuration window appears.

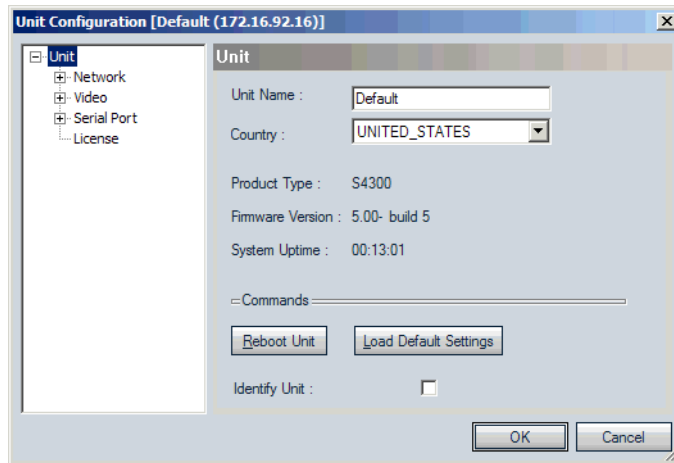
## Setting the Device Name and Country of Operation

It is recommended to give a meaningful name to each device, to help maintenance and debugging.

You must assign the proper country of operation to the device, so that it will comply to the DFS/TPC regulations, if applicable, respect the maximum EIRP, and use the proper set of frequency channels.

**To set the device name and country of operation:**

1. In the parameter tree of the Unit Configuration window, click **Unit**.



2. In the **Unit Name** box, assign a meaningful name to the device.
3. In the **Country** list, select the country of operation of the device.
4. In the confirmation window that appears, click **Yes**.

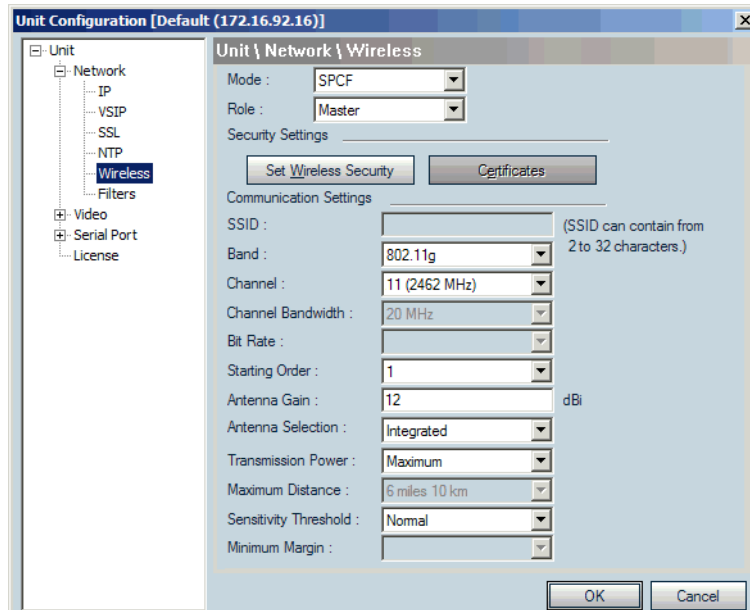
## Setting Wireless Parameters

The set of wireless values to apply to the two S4300 devices vary depending on the wireless cell; for an illustration of the application, see page 73.



**To set the wireless parameters:**

1. In the parameter tree of the Unit Configuration window, expand the **Network** structure, then click **Wireless**.



2. In the **Mode** list, select **SPCF** for both devices.
3. In the **Role** list, select **Master** for both devices.
4. In the **Band** list, select a frequency band. You must select the same value for both devices.
5. In the **Channel** list, select a frequency channel. The channels must be different for the two S4300 devices. You can also select **Auto** for the automatic selection.

**Tip:** To simplify channel management, especially if your system involves colocated cells, you should manually assign a channel to the S4300, not use the automatic channel selection.

Once the devices are installed in their final location, you should perform a site survey to select the proper frequency channel. For the procedure, see page 149.

6. If necessary in the 4.9 GHz band, change the bandwidth in the **Channel Bandwidth** list.
7. In a DFS context with automatic channel selection, enter in the **Starting Order** list a sequence number to delay its startup. This value must be different for each wireless cell. For more information about the starting order, see page 134.

8. If you are using an external antenna:
    - a. Enter its gain in the **Antenna Gain** box.
- Note: Providing a gain lower than the actual gain of the antenna you are using is prohibited.
- b. Select **External** in the **Antenna Selection** list.
  9. If you use the integrated antenna, check that the proper value is displayed in the **Antenna Gain** box; the gain is 8.5 dBi in the 2.4 GHz band and 12 dBi in the 4.9 GHz and 5 GHz bands.
  10. Set the wireless passkey to the value common to all devices in a cell. For the procedure, see next:
    - ☐ For S4300\_1, use the value given in Cell1.
    - ☐ For S4300\_2, use the value given in Cell2. The wireless passkey must be different for the two S4300 devices.

#### To set the wireless passkey:

1. In the Wireless pane, click **Set Wireless Security**.

The Set Wireless Security window appears.

2. In the **Format** list, select the format of the passkey: **Text (ASCII)** or **Hexadecimal**.

3. In the **Passkey** box, enter the new passkey (case-sensitive).

The user-supplied passkey must be unique and have exactly 16 characters if the format is Text, or 32 digits if Hexadecimal. For the wireless connection to be secure, do not enter a known name (like a street name), but instead use a mix of digits and letters. Do not disclose the passkey. The connection security is based on the secrecy and uniqueness of the passkey.

4. In the **Confirmation** box, enter again the passkey.
5. To set the wireless passkey to its default value, click **Reset**.
6. On a master device, to apply the new password to all associated devices:
  - a. Ensure that **Apply changes to connected clients/slaves** is checked.
  - b. Click **OK**.

Note: The wireless passkey of the master will be changed only when you click OK in the Unit Configuration window.

The Changing Wireless Passkey window appears.

- c. When the procedure is finished, click **Close**.
7. In the Set Wireless Security window, click **OK**.
  8. In the Unit Configuration window, click **OK**.
  9. In the Warning! window that appears, click **Yes** to save the new parameters.
  10. In the confirmation window that appears, click **OK**.

The device reboots with its new wireless configuration.

## Checking Communication

Using SConfigurator, ensure that the master device and its slaves communicate well together.

### To check communication:

1. If required, power up all the devices making up the system.
2. In the Units tab in SConfigurator, ensure that the associated devices are hierarchically positioned under the master.
3. In the Network > Wireless > Link Status pane of the Unit Configuration window of the master, ensure that the associated devices are in the Clients/Slaves list.
4. Ensure that there is end-to-end video transmission in the lab before installing the devices in their final locations.

# Installing the System

After ensuring that all devices are communicating properly in a lab, you can install the S4300 devices in their final location. Depending on your setup, you can install external antennas on the devices.

**Note:** When installing colocated wireless systems, take into account the distance limitations listed on page 29.

## Mounting a Device on a Pole or Wall



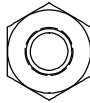
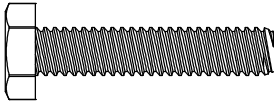
A point-to-point repeater is made up of two devices installed back to back and connected together with an outdoor Ethernet cable.

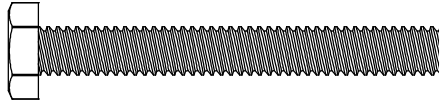
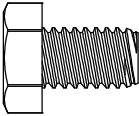
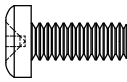
You can install an S4300 on a wall or pole using a mounting assembly set that is included in your shipment. The mounting assembly set includes:

- A mounting bracket
- A pole/wall pivot mount
- A pole clamp
- Two stainless steel straps

**Note:** You must install the mounting assembly on the S4300. It is required to properly mount and securely ground the wireless device.

The following fasteners are also part of the set:

Item	Description	Scale Drawing
1	Lock washers for the pole clamp (2) and the pole/wall mount pivot (2)	
2	Lock washers for the mounting bracket (4)	
3	Nuts for the pole clamp (2) and the pole/wall mount pivot (2)	
4	Hex screws (7/16 inch) for the pole/wall mount pivot (2)	

Item	Description	Scale Drawing
5	Hex screws (7/16 inch) for the pole clamp (2)	 <p>Not a scale drawing. Real length is 3.5 inches (89 mm).</p>
6	Hex screw (0.5 inch) for the ground lug (1)	
7	Screws (Phillips) for the mounting bracket (4)	

To install the mounting assembly, you need the following equipment:

- Phillips #2 screwdriver
- Slotted screwdriver
- 0.5-inch (13-mm) wrench
- 7/16-inch (11-mm) wrench
- Four screws if the device is installed on a wall

The pole diameter can vary from 1.0 to 6.5 inches (2.55 to 16.5 cm).

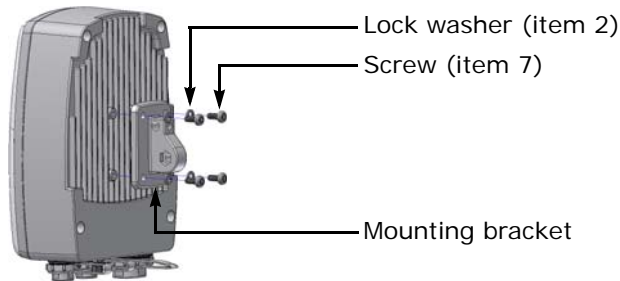
**Warning:** When installing colocated wireless systems, you have to take into account the distance limitations listed on page 29.

Always mount the device with the mating connectors pointing downwards.

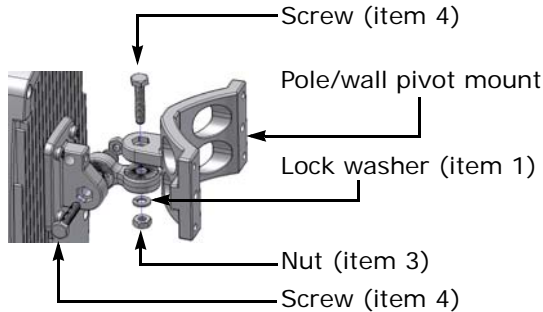
**Note:** If you are not installing a high-gain antenna, position the device so that its integrated antenna has a clear RF line of sight with the antennas of the facing devices.

**To mount an S4300 on a pole or wall:**

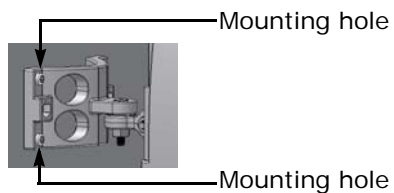
1. Install the mounting bracket on the rear of the device with a Phillips screwdriver, using the four screws (item 7) and the four lock washers (item 2). The recommended torque is 23 lbf-inch (2.6 N-m).



2. Attach the pole/wall pivot mount to the mounting bracket with a 7/16-inch (11-mm) wrench, using the two screws (item 4), two lock washers (item 1), and two nuts (item 3). The recommended torque is 70 lbf-inch (7.9 N-m).

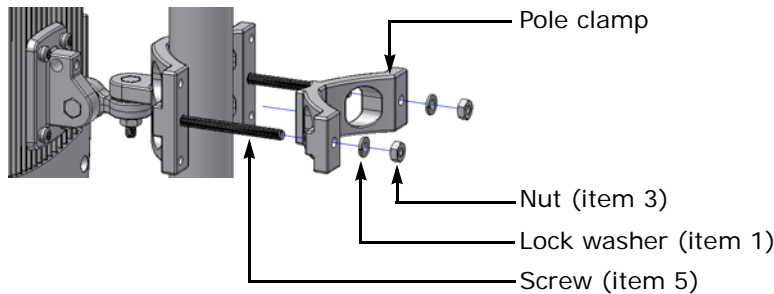


3. To install the device on a wall, use four screws (not supplied) in the four mounting holes located at the ends of the pole/wall pivot mount.

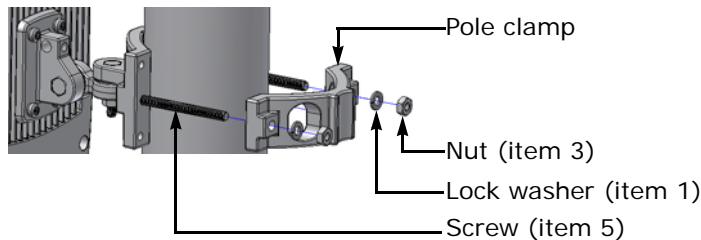


## 5: Configuring and Installing a Point-to-Point Repeater

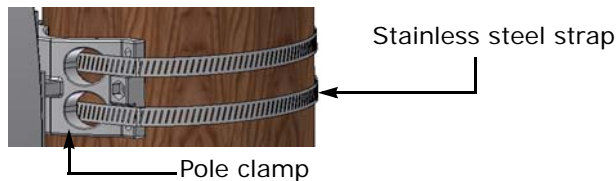
4. To install the device on a small pole (1–2.25 inch, or 2.55–5.7 cm diameter), position the device and the pole clamp the following way, then use a 7/16-inch (11-mm) wrench to put in place the two screws (item 5) with two nuts (item 3) and two lock washers (item 1). The recommended torque is 70 lbf-inch (7.9 N-m).



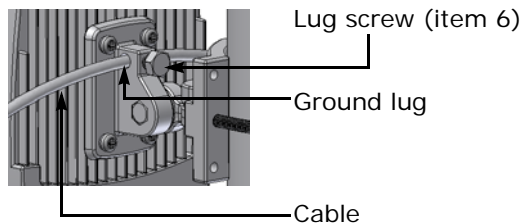
5. To install the device on a pole with a 2.25–3.25 inch diameter (5.7–8.25 cm), position the device and the pole clamp the following way, then use a 7/16-inch (11-mm) wrench to put in place the two screws (item 5) with two nuts (item 3) and two lock washers (item 1). The recommended torque is 70 lbf-inch (7.9 N-m).



6. To install the device on a pole with a 4.5–6.5 inch diameter (11.4–16.5 cm), use the supplied stainless steel straps and a slotted screwdriver.



7. Connect the device to the ground by inserting a copper cable into the ground lug, then screw in the lug screw (item 6) using a 0.5-inch (13-mm) wrench. Use a large diameter wire (minimum AWG 10; maximum AWG 1), and make it as short as possible. Then ground the cable.



8. To properly fuse the power supplied to the wireless device, install a fuse between the power source and the power cable. The fuse must have the following ratings: UL Listed, 250V, 2.5A, Fast-Acting.
9. Repeat step 1 to step 8 for the second device.
10. Ensure that the two devices making up the repeater are installed back to back.
11. If required, install external antennas on the devices (see page 88).

**Tip:** If you are installing the S4300 equipment in a lightning prone environment or in a site where large AC mains power fluctuations are a common occurrence, add external surge protection to secure your equipment. For more information, see Appendix C on page 154.

**Tip:** If the S4300 is directly exposed to the sun in an environment likely to reach 122°F (50°C), install a sun shield. Otherwise, reduce the maximum operating temperature by 18°F (10°C) to protect the equipment; that is, without a sun shield, the maximum temperature should be 104°F (40°C).

12. Power the devices using the assembled power devices.

**Note:** Power supplies other than the approved ones (PS2440) require verification of operation with the S4300-RP before use.

If you are using a power supply other than the one supplied by Verint, you need to ensure that it has a minimum capacity of 1.6A (for 12V DC) or 25 VA (for 24V AC).

13. Connect the supplied outdoor Ethernet cable between the two devices.
14. To improve the signal level between the devices, use the antenna alignment utility from SConfigurator.

## Installing an External Antenna

If you bought a high gain antenna, install it after the S4300 is in place.

**Note:** You can only use antennas certified by Verint. For the list, see the “Compliance” appendix on page 183.

The antenna requires professional installation.

The installer must enter the proper antenna gain in the device so that the transmission power is automatically adjusted. It is the responsibility of the installer to ensure that the proper antenna gain is configured. For fixed point-to-point applications in the 5.725 GHz–5.850 GHz in USA and Canada, 19 dBi and 23 dBi antennas can be used without transmission power reduction. It is the responsibility of the installer to ensure that the system is used exclusively for fixed point-to-point operation.



An omni-directional antenna (ANT-WP8-49/5x product code) is available for installation on a master device that requires a 360° coverage. Use it if the following conditions are met:

- There is a short distance between the master and slave devices (less than 0.6 mile/1 km). A typical use is in parking lots.
- At least three slaves are connected to the master.
- The antennas of the slaves point towards the omni-directional antenna and are in its vertical coverage zone (vertical beamwidth of 14°).
- The omni-directional antenna is installed vertically, without any tilt.

### To install an external antenna:

1. Install the antenna above the S4300 device. If you bought your antenna from Verint, use the supplied pole mount bracket.
2. Remove the cap from the antenna connector on the S4300.
3. Screw the SMA connector of the antenna cable to the antenna connector on the S4300 and tighten it with a 0.25-inch (0.6 centimeter) wrench.

**Warning:** Do not over-tighten to avoid damaging the connector. The recommended torque is 8 lbf-inch (100 N-cm). You could use a calibrated SMA torque wrench (for instance, from the Pasternack company, available at [www.pasternack.com](http://www.pasternack.com)).

Never leave the antenna connector without either the cap or the SMA connector. The antenna connector must be terminated to avoid damaging the device radio.

4. Apply two or three layers of electrical tape around all RF connections.  
The antenna cable and connectors are weather-tight; however, vibration caused by the wind will over time loosen the connectors and reduce the efficiency of the gaskets. The electrical tape will prevent this situation.
5. With SConfigurator, enter the new antenna gain and change the antenna selection from Integrated to External.
6. Carefully align the antenna with those of the other devices so that they have a clear RF line of sight.
7. To improve the signal level between both devices, use the antenna alignment utility from SConfigurator.

# 6

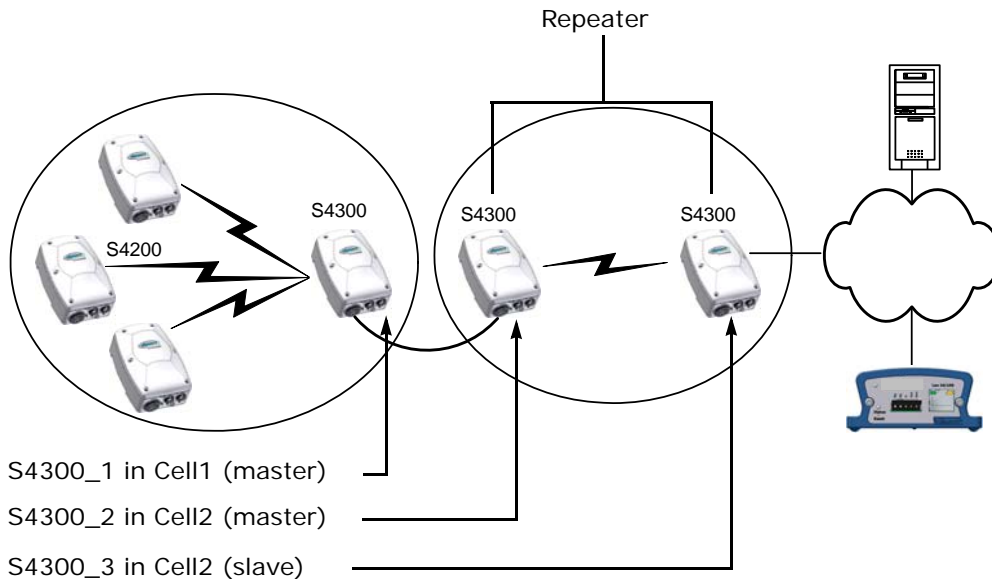
## Configuring and Installing a Point-to-Multipoint Repeater

The steps required to prepare your devices for point-to-multipoint repeater operation are:

1. Configuring and installing the S4200 transmitters. For the procedure, refer to the *Nextiva S4200 Series User Guide*.
2. Assembling the power devices.
3. Configuring the two S4300 devices part of the repeater (S4300-RP) and the S4300 access point connected to the LAN, one at a time. Shut down a device before configuring the next one.
4. Installing the S4300-RP.
5. Installing the S4300 access point. For the procedure, see page 48.
6. If required, installing an external antenna.

## Presenting the Application

A point-to-multipoint repeater is a range extender for wireless links, when you need to retransmit the signals coming from S4200 transmitters towards the Ethernet LAN. Use the S4300-RP (made up of two S4300 devices) to create this repeater. The application also requires an S4300 access point.



The repeater is made up of S4300\_2 and S4300\_3. S4300\_1 is an access point. All devices in this setup must be in the same IP subnet.

**Note:** Prior to deployment in the field, this wireless device requires configuration and testing.

## Connecting Power

The S4300-RP uses 12V DC or 24V AC for power. It is strongly recommended to connect power in a lab.

**Warning:** To avoid material damages, you must never power any two devices while their antennas are facing one another with a distance of less than 10 feet (3 meters).

Use the supplied power cable to power the devices.

**Note:** CE and FCC compliance testing has been performed with the MTA572415 (CE 24V AC) and MA572416 (24V AC North America) power supplies respectively. They correspond to the PS2440 power supply offered as an option by Verint.

Power supplies other than the approved ones require verification of operation with the S4300 before use.

If you are using a power supply other than the one supplied by Verint, you need to ensure that it has a minimum capacity of 1.6A (for 12V DC) or 25 VA (for 24V AC).

**To power the device:**

1. Plug the power cable on the main connector of the device.
2. In 12V DC, connect each power wire of the power cable to the corresponding wire of the power supply: the red wire to the input (+) wire and the black wire to the ground wire (-). For more information, refer to the power supply documentation.
3. In 24V AC, connect each power wire of the supplied cable to a wire on the power supply. Both wires are used for power.
4. Connect the electrical plug into the outlet.

## Configuring the Application

Device configuration requires the use of the proprietary SConfigurator tool. Its latest version is included on the Verint web site ([www.verint.com/manuals](http://www.verint.com/manuals)). You need to copy its executable file (SConfigurator.exe) to the hard disk of your computer.

It is strongly recommended to configure the S4300-RP in a lab.

Configuring each device making up the point-to-multipoint repeater involves the following sequence of steps:

**Note:** Never power more than one S4300 device at a time during the configuration process.

1. Setting the network parameters.
2. Setting the device name and country of operation.
3. Setting the wireless parameters.
4. Checking the communication between the devices.

For any other configuration task or for more information about the parameters, refer to the *Verint SConfigurator User Guide*.

## Setting Network Parameters

The first step in configuring an S4300 device is to provide a typical initial configuration of its network parameters (including its IP address) to ensure compatibility with an existing network.

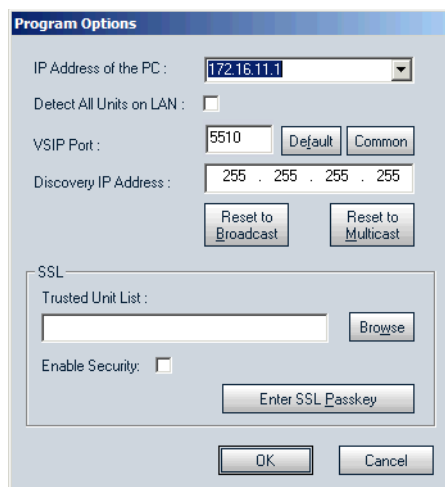
**Note:** To work properly, devices on the same network must have unique IP addresses. The device will not prevent you from entering a duplicate address. However, its system status LED will turn to flashing red (1-second interval); then the device will use its default address. You then need to configure it with a proper IP address.

### To set the initial network parameters:

1. Ensure that the device is powered.
2. Write down the serial numbers of the devices in a safe place.
3. Plug an Ethernet cable between the network (RJ-45) connector on the device and the network or a computer.

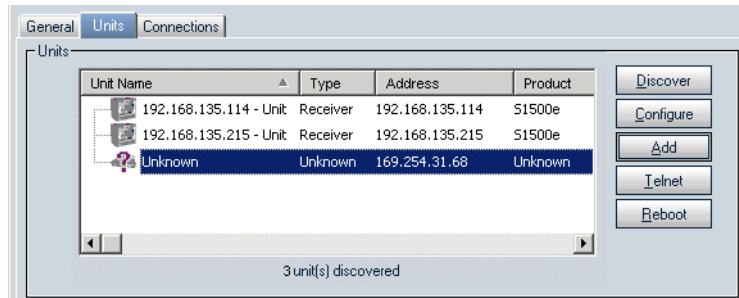
**Note:** The maximum length of this Ethernet cable is 328 feet (100 meters).

4. Start SConfigurator by double-clicking SConfigurator.exe on your hard disk. The SConfigurator window appears.
5. In the General tab, click **Program Options**. The Program Options window appears.

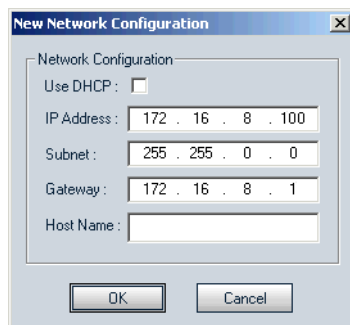


6. Check **Detect All Units on LAN**.
7. Ensure that the **VSIP Port** is 5510; otherwise, click **Default**.
8. Ensure that the **Discovery IP Address** is 255.255.255.255; otherwise, click **Reset to Broadcast**.
9. Click **OK**.

10. Select the **Units** tab, then click **Discover**. A device of type “Unknown” with a 169.254.X.Y IP address appears in the list; it corresponds to your new device. This default IP address is based on the APIPA (Automatic Private IP Addressing) addressing scheme. X and Y are relative to the MAC (Media Access Control) address of the device; for more information about APIPA, see page 152.



11. Select the unknown device, then click **Configure**.
12. In the Reconfigure unit? confirmation window, click **Yes**. The New Network Configuration window appears.



13. If you have a DHCP (Dynamic Host Configuration Protocol) server on your network, check **Use DHCP**. Otherwise, enter the IP address, subnet mask, and gateway of the device, as provided by your network administrator.

For more information about DHCP, see page 152.

14. Click **OK**.

The device reboots with its new network configuration.

15. In the Units tab, click **Discover** to update the list of devices.

The new S4300 device appears.

16. Select the device, then click **Configure**.

The Unit Configuration window appears.

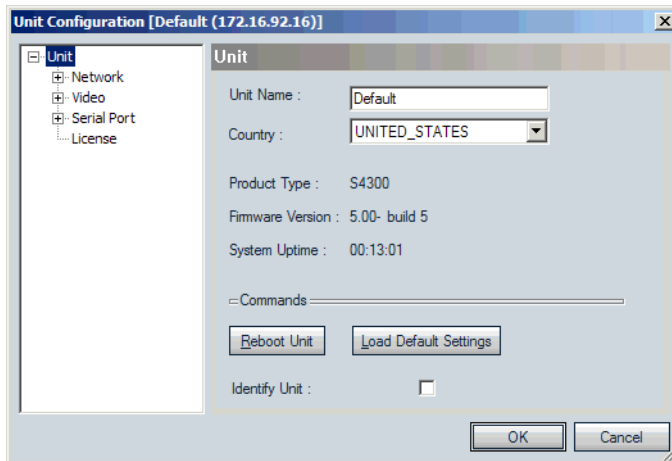
## Setting the Device Name and Country of Operation

It is recommended to give a meaningful name to each device, to help maintenance and debugging.

You must assign the proper country of operation to the device, so that it will comply to the DFS/TPC regulations, if applicable, respect the maximum EIRP, and use the proper set of frequency channels.

**To set the device name and country of operation:**

1. In the parameter tree of the Unit Configuration window, click **Unit**.



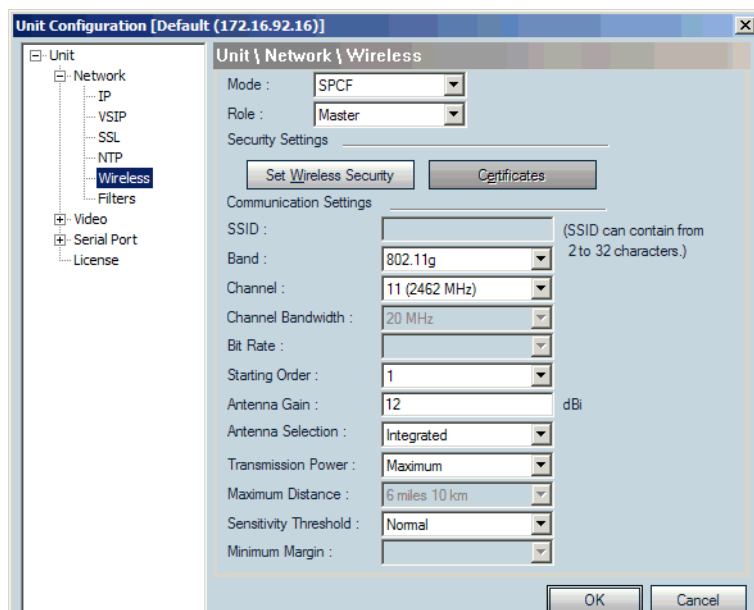
2. In the **Unit Name** box, assign a meaningful name to the device.
3. In the **Country** list, select the country of operation of the device.
4. In the confirmation window that appears, click **Yes**.

## Setting Wireless Parameters

The set of wireless values to apply to the two S4300 devices making up the repeater vary depending on the wireless cell; for an illustration of the application, see page 91. The repeater is made up of S4300\_2 and S4300\_3. S4300\_1 is an access point; for more information about its configuration, see Chapter 3 on page 39.

**To set the wireless parameters of the three S4300 devices forming the point-to-multipoint repeater:**

1. In the parameter tree of the Unit Configuration window, expand the **Network** structure, then click **Wireless**.



2. In the **Mode** list, select **SPCF** for all devices.
3. In the **Role** list, select **Master** for S4300\_1 and S4300\_2; select **Slave** for S4300\_3.
4. In the **Band** list, select the desired frequency band:
  - For S4300\_1, select the same frequency band as the S4200 transmitters.
  - For S4300\_2 and S4300\_3, select a frequency band; it can be the same as in S4300\_1 or a different one.
5. For S4300\_1 and S4300\_2 (masters), select a frequency channel in the **Channel** list. The channels must be different for the two devices. You can also select **Auto** for the automatic selection.

**Tip:** To simplify channel management, especially if your system involves colocated cells, you should manually assign a channel to the S4300, not use the automatic channel selection.

Once the devices are installed in their final location, you should perform a site survey to select the proper frequency channel. For the procedure, see page 149.

6. If necessary in the 4.9 GHz band, change the bandwidth in the **Channel Bandwidth** list.
7. For S4300\_3 (slave), select the data rate at which the wireless cell operates in the **Bit Rate** list.



## 6: Configuring and Installing a Point-to-Multipoint Repeater

8. For S4300\_1 and S4300\_2 (masters) in a DFS context with automatic channel selection, enter in the **Starting Order** list a sequence number to delay its startup. This number must be different for each wireless cell (for example, 1 for S4300\_1 and 2 for S4300\_2). For more information about the starting order, see page 134.
  9. If you are using an external antenna:
    - a. Enter its gain in the **Antenna Gain** box.
- Note:** Providing a gain lower than the actual gain of the antenna you are using is prohibited.
- b. Select **External** in the **Antenna Selection** list.
  10. If you use the integrated antenna, check that the proper value is displayed in the **Antenna Gain** box; the gain is 8.5 dBi in the 2.4 GHz band and 12 dBi in the 4.9 GHz and 5 GHz bands.
  11. Set the wireless passkey to the value common to all devices in the wireless cell. For the procedure, see next.
    - ☐ For S4300\_1, use the value given in Cell1 to the S4200 transmitters.
    - ☐ For S4300\_2 and S4300\_3, use the same value, but different than the passkey in Cell1.

### To set the wireless passkey:

1. In the Wireless pane, click **Set Wireless Security**.

The Set Wireless Security window appears.

**Set Wireless Security**

Authentication

WPA Authentication Method : WPA-PSK

WPA Negotiation Timeout : 45 second(s)

WPA Reauthentication Period : 1 day(s)

WPA EAP Login Name : stef

WPA EAP Password :

Confirmation Password :

Encryption

Encryption Type : AES-OCB

Format : ☐ Text (ASCII) ☒ Hexadecimal

Passkey :

Confirmation :

The key must contain exactly 32 hexadecimal digits (0-9 and A-F).

☐ Apply changes to connected clients / slaves.

2. In the **Format** list, select the format of the passkey: **Text (ASCII)** or **Hexadecimal**.

3. In the **Passkey** box, enter the new passkey (case-sensitive).

The user-supplied passkey must be unique and have exactly 16 characters if the format is Text, or 32 digits if Hexadecimal. For the wireless connection to be secure, do not enter a known name (like a street name), but instead use a mix of digits and letters. Do not disclose the passkey. The connection security is based on the secrecy and uniqueness of the passkey.

4. In the **Confirmation** box, enter again the passkey.
5. To set the wireless passkey to its default value, click **Reset**.
6. On a master device, to apply the new password to all associated devices:
  - a. Ensure that **Apply changes to connected clients/slaves** is checked.
  - b. Click **OK**.

**Note:** The wireless passkey of the master will be changed only when you click OK in the Unit Configuration window.

The Changing Wireless Passkey window appears.

- c. When the procedure is finished, click **Close**.
7. In the Set Wireless Security window, click **OK**.
8. In the Unit Configuration window, click **OK**.
9. In the Warning! window that appears, click **Yes** to save the new parameters.
10. In the confirmation window that appears, click **OK**.

The device reboots with its new wireless configuration.

## Checking Communication

Using SConfigurator, ensure that the master device and its slaves communicate well together.

### To check communication:

1. If required, power up all the devices making up the system.
2. In the Units tab in SConfigurator, ensure that the associated devices are hierarchically positioned under the master.
3. In the Network > Wireless > Link Status pane of the Unit Configuration window of the master, ensure that the associated devices are in the Clients/Slaves list.
4. Ensure that there is end-to-end video transmission in the lab before installing the devices in their final locations.

# Installing the System

After ensuring that all devices are communicating properly in a lab, you can install the S4300 devices in their final location. Depending on your setup, you can install external antennas on the devices.

**Note:** When installing colocated wireless systems, take into account the distance limitations listed on page 29.

## Mounting a Device on a Pole or Wall



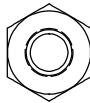
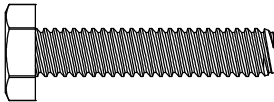
A point-to-multipoint repeater is made up of two devices installed back to back and connected together with an outdoor Ethernet cable.

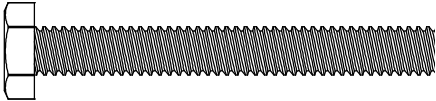
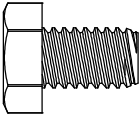
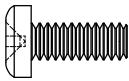
You can install an S4300 on a wall or pole using a mounting assembly set that is included in your shipment. The mounting assembly set includes:

- A mounting bracket
- A pole/wall pivot mount
- A pole clamp
- Two stainless steel straps

**Note:** You must install the mounting assembly on the S4300. It is required to properly mount and securely ground the wireless device.

The following fasteners are also part of the set:

Item	Description	Scale Drawing
1	Lock washers for the pole clamp (2) and the pole/wall mount pivot (2)	
2	Lock washers for the mounting bracket (4)	
3	Nuts for the pole clamp (2) and the pole/wall mount pivot (2)	
4	Hex screws (7/16 inch) for the pole/wall mount pivot (2)	

Item	Description	Scale Drawing
5	Hex screws (7/16 inch) for the pole clamp (2)	  Not a scale drawing. Real length is 3.5 inches (89 mm).
6	Hex screw (0.5 inch) for the ground lug (1)	
7	Screws (Phillips) for the mounting bracket (4)	

To install the mounting assembly, you need the following equipment:

- Phillips #2 screwdriver
- Slotted screwdriver
- 0.5-inch (13-mm) wrench
- 7/16-inch (11-mm) wrench
- Four screws if the device is installed on a wall

The pole diameter can vary from 1.0 to 6.5 inches (2.55 to 16.5 cm).

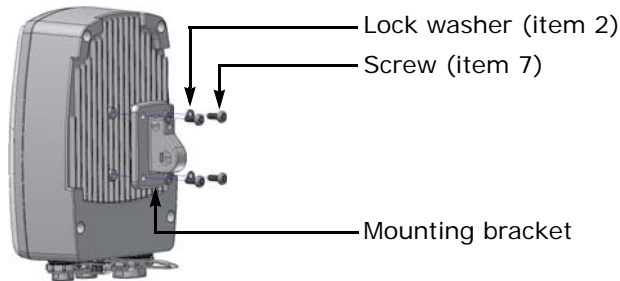
**Warning:** When installing colocated wireless systems, you have to take into account the distance limitations listed on page 29.

Always mount the device with the mating connectors pointing downwards.

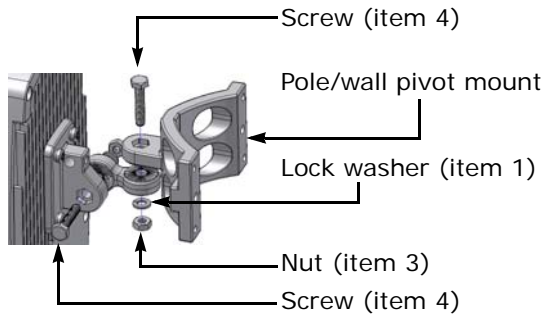
**Note:** If you are not installing a high-gain antenna, position the device so that its integrated antenna has a clear RF line of sight with the antennas of the facing devices.

**To mount an S4300 on a pole or wall:**

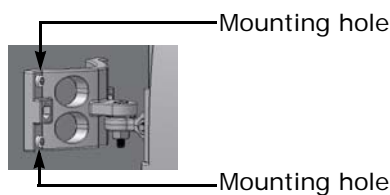
1. Install the mounting bracket on the rear of the device with a Phillips screwdriver, using the four screws (item 7) and the four lock washers (item 2). The recommended torque is 23 lbf-inch (2.6 N-m).



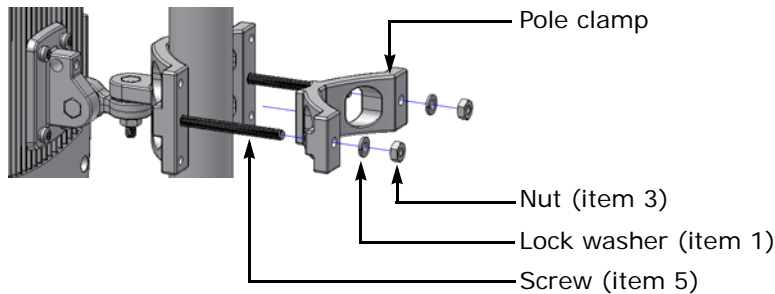
2. Attach the pole/wall pivot mount to the mounting bracket with a 7/16-inch (11-mm) wrench, using the two screws (item 4), two lock washers (item 1), and two nuts (item 3). The recommended torque is 70 lbf-inch (7.9 N-m).



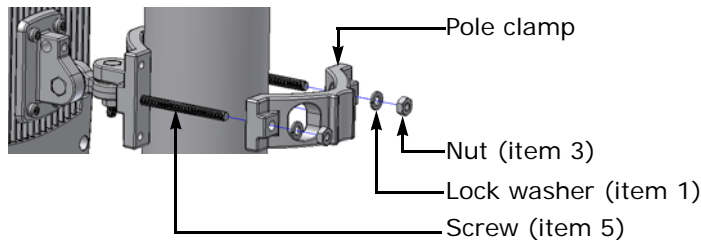
3. To install the device on a wall, use four screws (not supplied) in the four mounting holes located at the ends of the pole/wall pivot mount.



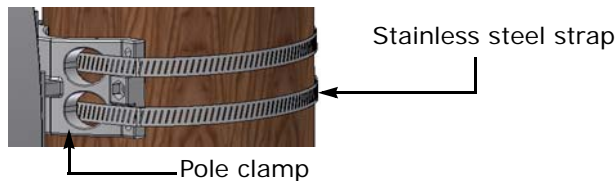
4. To install the device on a small pole (1–2.25 inch, or 2.55–5.7 cm diameter), position the device and the pole clamp the following way, then use a 7/16-inch (11-mm) wrench to put in place the two screws (item 5) with two nuts (item 3) and two lock washers (item 1). The recommended torque is 70 lbf-inch (7.9 N-m).



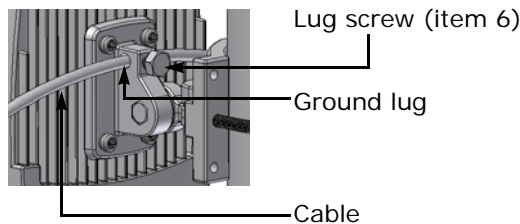
5. To install the device on a pole with a 2.25–3.25 inch diameter (5.7–8.25 cm), position the device and the pole clamp the following way, then use a 7/16-inch (11-mm) wrench to put in place the two screws (item 5) with two nuts (item 3) and two lock washers (item 1). The recommended torque is 70 lbf-inch (7.9 N-m).



6. To install the device on a pole with a 4.5–6.5 inch diameter (11.4–16.5 cm), use the supplied stainless steel straps and a slotted screwdriver.



7. Connect the device to the ground by inserting a copper cable into the ground lug, then screw in the lug screw (item 6) using a 0.5-inch (13-mm) wrench. Use a large diameter wire (minimum AWG 10; maximum AWG 1), and make it as short as possible. Then ground the cable.



8. To properly fuse the power supplied to the wireless device, install a fuse between the power source and the power cable. The fuse must have the following ratings: UL Listed, 250V, 2.5A, Fast-Acting.
9. Repeat step 1 to step 8 for the second device.
10. If required, install external antennas on the devices (see next).

**Tip:** If you are installing the S4300 equipment in a lightning prone environment or in a site where large AC mains power fluctuations are a common occurrence, add external surge protection to secure your equipment. For more information, see Appendix C on page 154.

**Tip:** If the S4300 is directly exposed to the sun in an environment likely to reach 122°F (50°C), install a sun shield. Otherwise, reduce the maximum operating temperature by 18°F (10°C) to protect the equipment; that is, without a sun shield, the maximum temperature should be 104°F (40°C).

11. Power the devices using the assembled power devices.

**Note:** Power supplies other than the approved ones (PS2440) require verification of operation with the S4300-RP before use.

If you are using a power supply other than the one supplied by Verint, you need to ensure that it has a minimum capacity of 1.6A (for 12V DC) or 25 VA (for 24V AC).

12. Install the S4300 access point in its final location; for the procedure, see page 48.
13. Connect the supplied outdoor Ethernet cable between the S4300 access point (S4300\_1 in the illustration on page 95) and the master device in the repeater (S4300\_2).
14. To improve the signal level between the devices, use the antenna alignment utility from SConfigurator.

## Installing an External Antenna

If you bought a high gain antenna, install it after the S4300 is in place.

**Note:** You can only use antennas certified by Verint. For the list, see the “Compliance” appendix on page 183.

The antenna requires professional installation.

The installer must enter the proper antenna gain in the device so that the transmission power is automatically adjusted. It is the responsibility of the installer to ensure that the proper antenna gain is configured. For fixed point-to-point applications in the 5.725 GHz–5.850 GHz in USA and Canada, 19 dBi and 23 dBi antennas can be used without transmission power reduction. It is the responsibility of the installer to ensure that the system is used exclusively for fixed point-to-point operation.

An omni-directional antenna (ANT-WP8-49/5x product code) is available for installation on a master device that requires a 360° coverage. Use it if the following conditions are met:

- There is a short distance between the master and slave devices (less than 0.6 mile/1 km). A typical use is in parking lots.
- At least three slaves are connected to the master.
- The antennas of the slaves point towards the omni-directional antenna and are in its vertical coverage zone (vertical beamwidth of 14°).
- The omni-directional antenna is installed vertically, without any tilt.

**To install an external antenna:**

1. Install the antenna above the S4300 device. If you bought your antenna from Verint, use the supplied pole mount bracket.
2. Remove the cap from the antenna connector on the S4300.
3. Screw the SMA connector of the antenna cable to the antenna connector on the S4300 and tighten it with a 0.25-inch (0.6 centimeter) wrench.

**Warning:** Do not over-tighten to avoid damaging the connector. The recommended torque is 8 lbf-inch (100 N-cm). You could use a calibrated SMA torque wrench (for instance, from the Pasternack company, available at [www.pasternack.com](http://www.pasternack.com)).

Never leave the antenna connector without either the cap or the SMA connector. The antenna connector must be terminated to avoid damaging the device radio.

4. Apply two or three layers of electrical tape around all RF connections.  
The antenna cable and connectors are weather-tight; however, vibration caused by the wind will over time loosen the connectors and reduce the efficiency of the gaskets. The electrical tape will prevent this situation.
5. With SConfigurator, enter the new antenna gain and change the antenna selection from Integrated to External.
6. Carefully align the antenna with those of the other devices so that they have a clear RF line of sight.
7. To improve the signal level between both devices, use the antenna alignment utility from SConfigurator.



# 7

## Configuring and Installing a Wireless Bridge Repeater

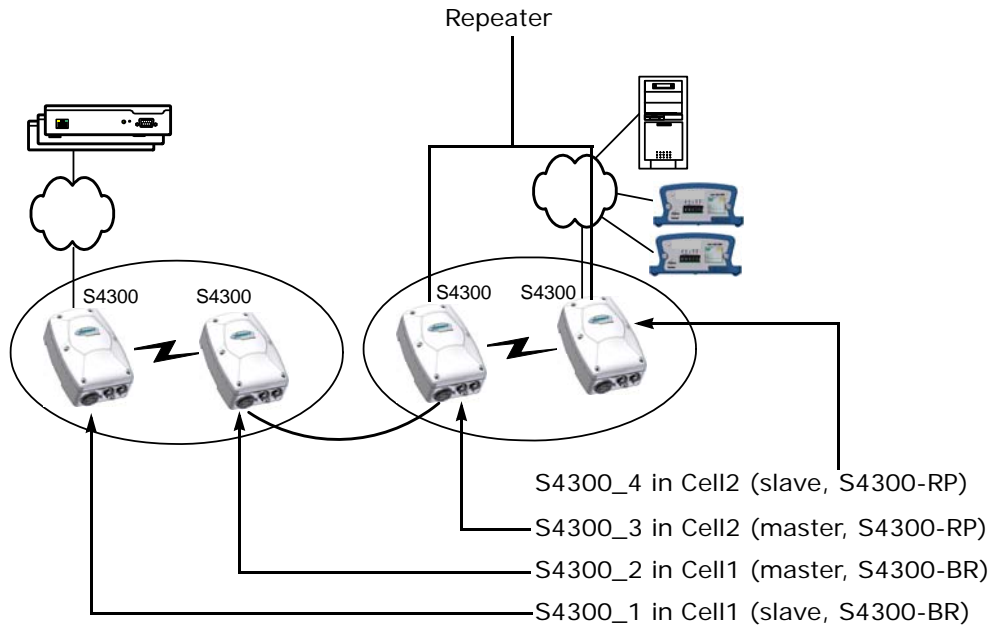
The steps required to prepare your devices for wireless bridge repeater operation are:

1. Assembling the power devices.
2. Configuring the two S4300 devices part of the repeater (S4300-RP) and the two devices part of the wireless bridge (S4300-BR), one at a time. Shut down a device before configuring the next one.
3. Installing the S4300-RP.
4. Installing the S4300-BR. For the procedure, see page 65.
5. If required, installing an external antenna.

# Presenting the Application

A wireless bridge repeater is used as a range extender to retransmit the signals exchanged by the two devices forming a wireless bridge. A typical context is when you cannot obtain an RF line of sight between the two devices forming the wireless bridge.

A wireless bridge repeater is made up of four devices: two for the repeater (S4300-RP product code) and two for the wireless bridge (S4300-BR product code). These devices are organized in two wireless cells.



Note: Prior to deployment in the field, this wireless device requires configuration and testing.

## Connecting Power

The S4300-RP uses 12V DC or 24V AC for power. It is strongly recommended to connect power in a lab.

Warning: To avoid material damages, you must never power any two devices while their antennas are facing one another with a distance of less than 10 feet (3 meters).

Use the supplied power cable to power the devices.

**Note:** CE and FCC compliance testing has been performed with the MTA572415 (CE 24V AC) and MA572416 (24V AC North America) power supplies respectively. They correspond to the PS2440 power supply offered as an option by Verint.

Power supplies other than the approved ones require verification of operation with the S4300 before use.

If you are using a power supply other than the one supplied by Verint, you need to ensure that it has a minimum capacity of 1.6A (for 12V DC) or 25 VA (for 24V AC).

### To power the device:

1. Plug the power cable on the main connector of the device.
2. In 12V DC, connect each power wire of the power cable to the corresponding wire of the power supply: the red wire to the input (+) wire and the black wire to the ground wire (-). For more information, refer to the power supply documentation.
3. In 24V AC, connect each power wire of the supplied cable to a wire on the power supply. Both wires are used for power.
4. Connect the electrical plug into the outlet.

## Configuring the Application

Device configuration requires the use of the proprietary SConfigurator tool. Its latest version is included on the Verint web site ([www.verint.com/manuals](http://www.verint.com/manuals)). You need to copy its executable file (SConfigurator.exe) to the hard disk of your computer.

It is strongly recommended to configure the S4300-RP in a lab.

Configuring each device making up the wireless bridge repeater involves the following sequence of steps:

**Note:** Never power more than one S4300 device at a time during the configuration process.

1. Setting the network parameters.
2. Setting the device name and country of operation.
3. Setting the wireless parameters.
4. Checking the communication between the devices.

For any other configuration task or for more information about the parameters, refer to the *Verint SConfigurator User Guide*.

## Setting Network Parameters

The first step in configuring an S4300 device is to provide a typical initial configuration of its network parameters (including its IP address) to ensure compatibility with an existing network.

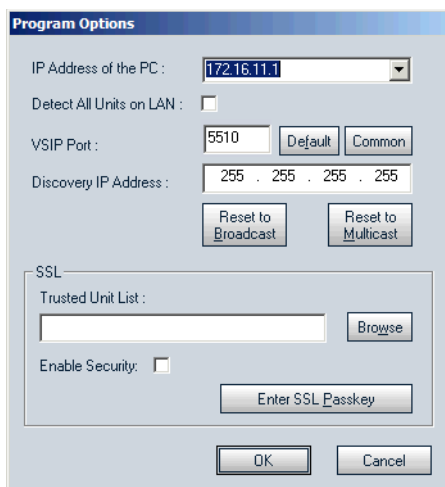
**Note:** To work properly, devices on the same network must have unique IP addresses. The device will not prevent you from entering a duplicate address. However, its system status LED will turn to flashing red (1-second interval); then the device will use its default address. You then need to configure it with a proper IP address.

### To set the initial network parameters:

1. Ensure that the device is powered.
2. Write down the serial numbers of the devices in a safe place.
3. Plug an Ethernet cable between the network (RJ-45) connector on the device and the network or a computer.

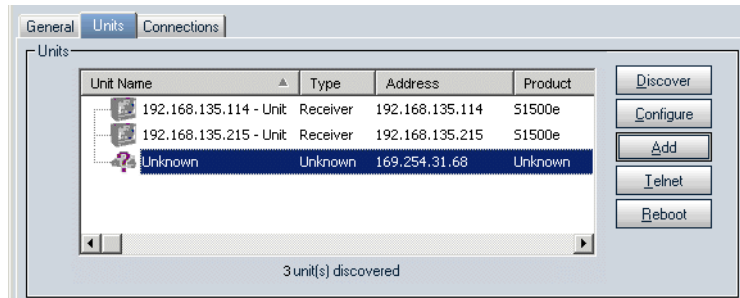
**Note:** The maximum length of this Ethernet cable is 328 feet (100 meters).

4. Start SConfigurator by double-clicking SConfigurator.exe on your hard disk. The SConfigurator window appears.
5. In the General tab, click **Program Options**. The Program Options window appears.

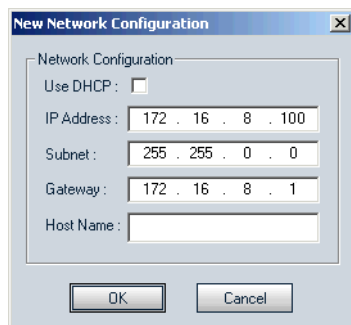


6. Check **Detect All Units on LAN**.
7. Ensure that the **VSIP Port** is 5510; otherwise, click **Default**.
8. Ensure that the **Discovery IP Address** is 255.255.255.255; otherwise, click **Reset to Broadcast**.
9. Click **OK**.

10. Select the **Units** tab, then click **Discover**. A device of type “Unknown” with a 169.254.X.Y IP address appears in the list; it corresponds to your new device. This default IP address is based on the APIPA (Automatic Private IP Addressing) addressing scheme. X and Y are relative to the MAC (Media Access Control) address of the device; for more information about APIPA, see page 152.



11. Select the unknown device, then click **Configure**.
12. In the Reconfigure unit? confirmation window, click **Yes**. The New Network Configuration window appears.



13. If you have a DHCP (Dynamic Host Configuration Protocol) server on your network, check **Use DHCP**. Otherwise, enter the IP address, subnet mask, and gateway of the device, as provided by your network administrator.

For more information about DHCP, see page 152.

14. Click **OK**.

The device reboots with its new network configuration.

15. In the Units tab, click **Discover** to update the list of devices.

The new S4300 device appears.

16. Select the device, then click **Configure**.

The Unit Configuration window appears.

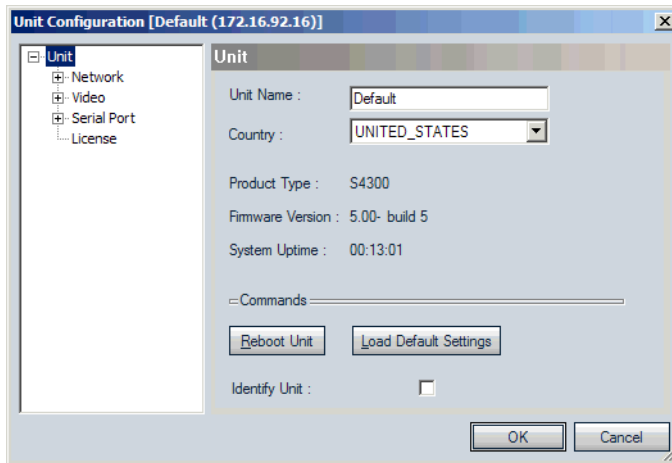
## Setting the Device Name and Country of Operation

It is recommended to give a meaningful name to each device, to help maintenance and debugging.

You must assign the proper country of operation to the device, so that it will comply to the DFS/TPC regulations, if applicable, respect the maximum EIRP, and use the proper set of frequency channels.

**To set the device name and country of operation:**

1. In the parameter tree of the Unit Configuration window, click **Unit**.



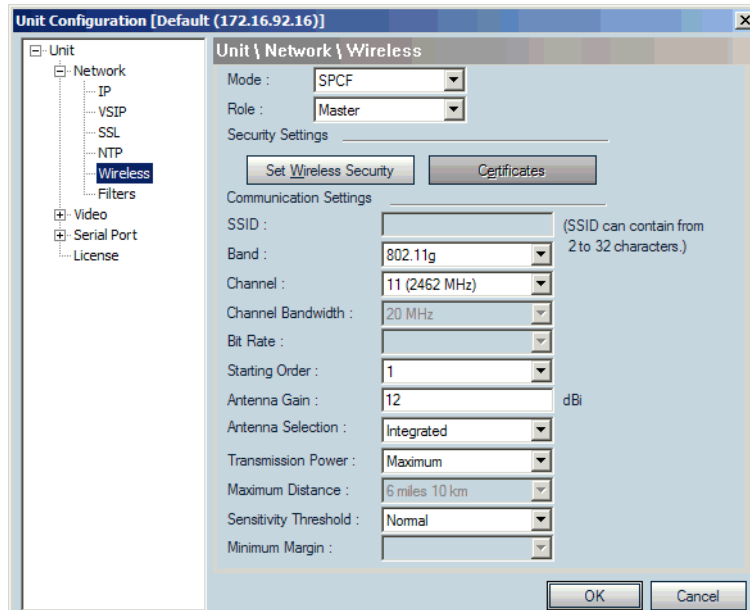
2. In the **Unit Name** box, assign a meaningful name to the device.
3. In the **Country** list, select the country of operation of the device.
4. In the confirmation window that appears, click **Yes**.

## Setting Wireless Parameters

The set of wireless values to apply to the two S4300 devices making up the repeater vary depending on the wireless cell; for an illustration of the application, see page 106. The repeater is made up of S4300\_2 and S4300\_3. The wireless bridge is S4300\_1 and S4300\_4; for its configuration, see page 114.

### To set the wireless parameters of the repeater and wireless bridge:

1. In the parameter tree of the Unit Configuration window, expand the **Network** structure, then click **Wireless**.



2. In the **Mode** list, select **SPCF** for all devices.
3. In the **Role** list, select **Master** for S4300\_2 and S4300\_3; select **Slave** for S4300\_1 and S4300\_4.
4. In the **Band** list, select the frequency band:
  - S4300\_1 and S4300\_2 must use the same band.
  - S4300\_3 and S4300\_4 must use the same band; it can be the same as in the other cell or a different band.
5. For S4300\_2 and S4300\_3 (masters), select a frequency channel in the **Channel** list. The channels must be different for the two devices. You can also select **Auto** for the automatic selection.

**Tip:** To simplify channel management, especially if your system involves colocated cells, you should manually assign a channel to the S4300, not use the automatic channel selection.

Once the devices are installed in their final location, you should perform a site survey to select the proper frequency channel. For the procedure, see page 149.

6. If necessary in the 4.9 GHz band, change the bandwidth in the **Channel Bandwidth** list.
7. For S4300\_1 and S4300\_4 (slaves), select the data rate at which the wireless cell operates in the **Bit Rate** list. These values do not need to be the same.

8. For S4300\_2 and S4300\_3 (masters) in a DFS context with automatic channel selection, enter in the **Starting Order** list a sequence number to delay its startup. This number must be different for each wireless cell (for example, 1 for S4300\_2 and 2 for S4300\_3). For more information about the starting order, see page 134.
  9. If you are using an external antenna:
    - a. Enter its gain in the **Antenna Gain** box.
- Note:** Providing a gain lower than the actual gain of the antenna you are using is prohibited.
- b. Select **External** in the **Antenna Selection** list.
  10. If you use the integrated antenna, check that the proper value is displayed in the **Antenna Gain** box; the gain is 8.5 dBi in the 2.4 GHz band and 12 dBi in the 4.9 GHz and 5 GHz bands.
  11. Set the wireless passkey to the value common to all devices in the wireless cell. For the procedure, see next.
    - ☐ For S4300\_1 and S4300\_2, use the same passkey.
    - ☐ For S4300\_3 and S4300\_4, use the same value, but different than the passkey in Cell1.

#### To set the wireless passkey:

1. In the Wireless pane, click **Set Wireless Security**.

The Set Wireless Security window appears.

**Set Wireless Security**

**Authentication**

WPA Authentication Method : WPA-PSK

WPA Negotiation Timeout : 45 second(s)

WPA Reauthentication Period : 1 day(s)

WPA EAP Login Name : stef

WPA EAP Password :

Confirmation Password :

**Encryption**

Encryption Type : AES-OCB

Format : ☐ Text (ASCII) ☒ Hexadecimal Reset

Passkey :

Confirmation :

The key must contain exactly 32 hexadecimal digits (0-9 and A-F).

☐ Apply changes to connected clients / slaves.

OK Cancel

2. In the **Format** list, select the format of the passkey: **Text (ASCII)** or **Hexadecimal**.



3. In the **Passkey** box, enter the new passkey (case-sensitive).

The user-supplied passkey must be unique and have exactly 16 characters if the format is Text, or 32 digits if Hexadecimal. For the wireless connection to be secure, do not enter a known name (like a street name), but instead use a mix of digits and letters. Do not disclose the passkey. The connection security is based on the secrecy and uniqueness of the passkey.

4. In the **Confirmation** box, enter again the passkey.
5. To set the wireless passkey to its default value, click **Reset**.
6. On a master device, to apply the new password to all associated devices:
  - a. Ensure that **Apply changes to connected clients/slaves** is checked.
  - b. Click **OK**.

Note: The wireless passkey of the master will be changed only when you click OK in the Unit Configuration window.

The Changing Wireless Passkey window appears.

- c. When the procedure is finished, click **Close**.
7. In the Set Wireless Security window, click **OK**.
  8. In the Unit Configuration window, click **OK**.
  9. In the Warning! window that appears, click **Yes** to save the new parameters.
  10. In the confirmation window that appears, click **OK**.

The device reboots with its new wireless configuration.

## Checking Communication

Using SConfigurator, ensure that the master device and its slaves communicate well together.

### To check communication:

1. If required, power up all the devices making up the system.
2. In the Units tab in SConfigurator, ensure that the associated devices are hierarchically positioned under the master.
3. In the Network > Wireless > Link Status pane of the Unit Configuration window of the master, ensure that the associated devices are in the Clients/Slaves list.
4. Ensure that there is end-to-end video transmission in the lab before installing the devices in their final locations.

# Installing the System

After ensuring that all devices are communicating properly in a lab, you can install the S4300 devices in their final location. Depending on your setup, you can install external antennas on the devices.

**Note:** When installing colocated wireless systems, take into account the distance limitations listed on page 29.

## Mounting a Device on a Pole or Wall



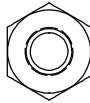
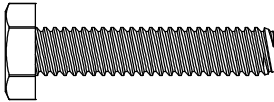
A wireless bridge repeater is made up of two devices installed back to back and connected together with an outdoor Ethernet cable.

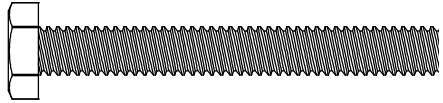
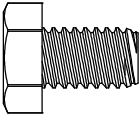
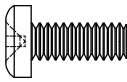
You can install an S4300 on a wall or pole using a mounting assembly set that is included in your shipment. The mounting assembly set includes:

- A mounting bracket
- A pole/wall pivot mount
- A pole clamp
- Two stainless steel straps

**Note:** You must install the mounting assembly on the S4300. It is required to properly mount and securely ground the wireless device.

The following fasteners are also part of the set:

Item	Description	Scale Drawing
1	Lock washers for the pole clamp (2) and the pole/wall mount pivot (2)	
2	Lock washers for the mounting bracket (4)	
3	Nuts for the pole clamp (2) and the pole/wall mount pivot (2)	
4	Hex screws (7/16 inch) for the pole/wall mount pivot (2)	

Item	Description	Scale Drawing
5	Hex screws (7/16 inch) for the pole clamp (2)	 <p>Not a scale drawing. Real length is 3.5 inches (89 mm).</p>
6	Hex screw (0.5 inch) for the ground lug (1)	
7	Screws (Phillips) for the mounting bracket (4)	

To install the mounting assembly, you need the following equipment:

- Phillips #2 screwdriver
- Slotted screwdriver
- 0.5-inch (13-mm) wrench
- 7/16-inch (11-mm) wrench
- Four screws if the device is installed on a wall

The pole diameter can vary from 1.0 to 6.5 inches (2.55 to 16.5 cm).

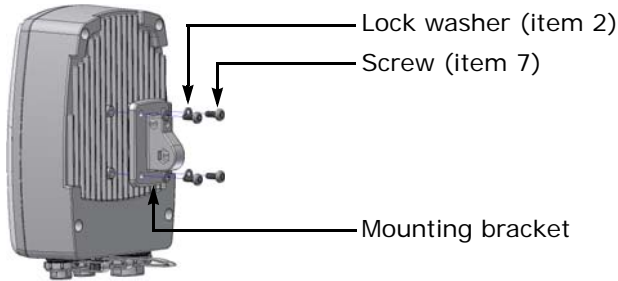
**Warning:** When installing colocated wireless systems, you have to take into account the distance limitations listed on page 29.

Always mount the device with the mating connectors pointing downwards.

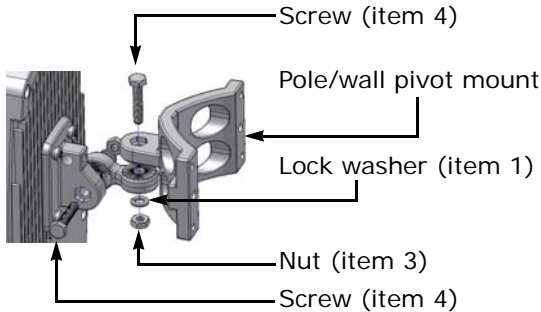
**Note:** If you are not installing a high-gain antenna, position the device so that its integrated antenna has a clear RF line of sight with the antennas of the facing devices.

**To mount an S4300 on a pole or wall:**

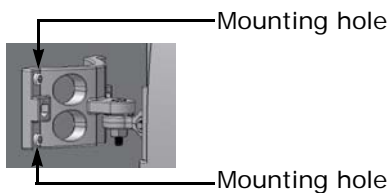
1. Install the mounting bracket on the rear of the device with a Phillips screwdriver, using the four screws (item 7) and the four lock washers (item 2). The recommended torque is 23 lbf-inch (2.6 N-m).



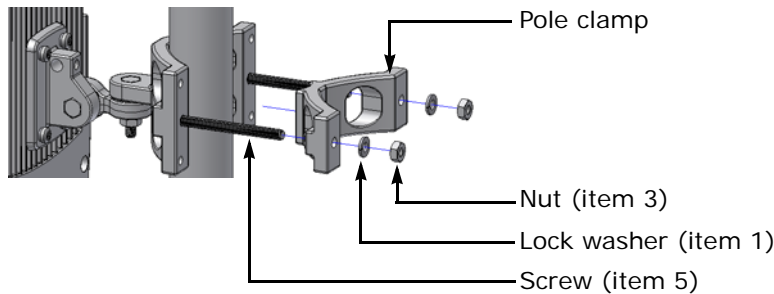
2. Attach the pole/wall pivot mount to the mounting bracket with a 7/16-inch (11-mm) wrench, using the two screws (item 4), two lock washers (item 1), and two nuts (item 3). The recommended torque is 70 lbf-inch (7.9 N-m).



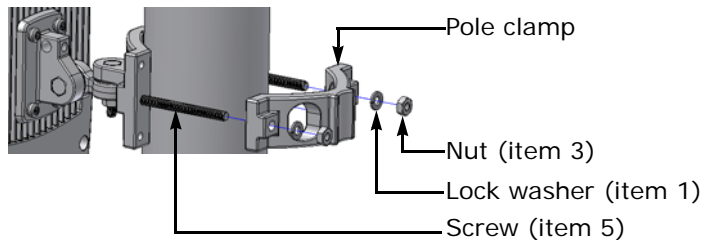
3. To install the device on a wall, use four screws (not supplied) in the four mounting holes located at the ends of the pole/wall pivot mount.



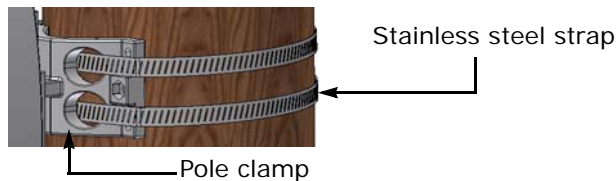
4. To install the device on a small pole (1–2.25 inch, or 2.55–5.7 cm diameter), position the device and the pole clamp the following way, then use a 7/16-inch (11-mm) wrench to put in place the two screws (item 5) with two nuts (item 3) and two lock washers (item 1). The recommended torque is 70 lbf-inch (7.9 N-m).



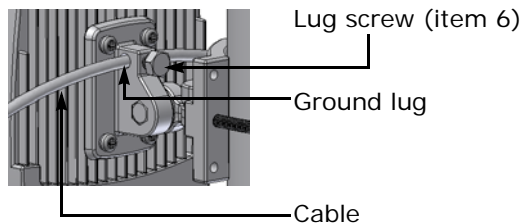
5. To install the device on a pole with a 2.25–3.25 inch diameter (5.7–8.25 cm), position the device and the pole clamp the following way, then use a 7/16-inch (11-mm) wrench to put in place the two screws (item 5) with two nuts (item 3) and two lock washers (item 1). The recommended torque is 70 lbf-inch (7.9 N-m).



6. To install the device on a pole with a 4.5–6.5 inch diameter (11.4–16.5 cm), use the supplied stainless steel straps and a slotted screwdriver.



7. Connect the device to the ground by inserting a copper cable into the ground lug, then screw in the lug screw (item 6) using a 0.5-inch (13-mm) wrench. Use a large diameter wire (minimum AWG 10; maximum AWG 1), and make it as short as possible. Then ground the cable.



8. To properly fuse the power supplied to the wireless device, install a fuse between the power source and the power cable. The fuse must have the following ratings: UL Listed, 250V, 2.5A, Fast-Acting.
9. Repeat step 1 to step 8 for the second device.
10. If required, install external antennas on the devices (see next).

**Tip:** If you are installing the S4300 equipment in a lightning prone environment or in a site where large AC mains power fluctuations are a common occurrence, add external surge protection to secure your equipment. For more information, see Appendix C on page 154.

**Tip:** If the S4300 is directly exposed to the sun in an environment likely to reach 122°F (50°C), install a sun shield. Otherwise, reduce the maximum operating temperature by 18°F (10°C) to protect the equipment; that is, without a sun shield, the maximum temperature should be 104°F (40°C).

11. Power the devices using the assembled power devices.

**Note:** Power supplies other than the approved ones (PS2440) require verification of operation with the S4300-RP before use.

If you are using a power supply other than the one supplied by Verint, you need to ensure that it has a minimum capacity of 1.6A (for 12V DC) or 25 VA (for 24V AC).

12. Install the wireless bridge; for more information, see page 65.
13. Connect the supplied outdoor Ethernet cable between the two master devices (S4300\_2 and S4300\_3 in the illustration on page 106).
14. To improve the signal level between the devices, use the antenna alignment utility from SConfigurator.

## Installing an External Antenna

If you bought a high gain antenna, install it after the S4300 is in place.

**Note:** You can only use antennas certified by Verint. For the list, see the “Compliance” appendix on page 183.

The antenna requires professional installation.

The installer must enter the proper antenna gain in the device so that the transmission power is automatically adjusted. It is the responsibility of the installer to ensure that the proper antenna gain is configured. For fixed point-to-point applications in the 5.725 GHz–5.850 GHz in USA and Canada, 19 dBi and 23 dBi antennas can be used without transmission power reduction. It is the responsibility of the installer to ensure that the system is used exclusively for fixed point-to-point operation.

An omni-directional antenna (ANT-WP8-49/5x product code) is available for installation on a master device that requires a 360° coverage. Use it if the following conditions are met:

- There is a short distance between the master and slave devices (less than 0.6 mile/1 km). A typical use is in parking lots.
- At least three slaves are connected to the master.
- The antennas of the slaves point towards the omni-directional antenna and are in its vertical coverage zone (vertical beamwidth of 14°).
- The omni-directional antenna is installed vertically, without any tilt.

### To install an external antenna:

1. Install the antenna above the S4300 device. If you bought your antenna from Verint, use the supplied pole mount bracket.
2. Remove the cap from the antenna connector on the S4300.
3. Screw the SMA connector of the antenna cable to the antenna connector on the S4300 and tighten it with a 0.25-inch (0.6 centimeter) wrench.

**Warning:** Do not over-tighten to avoid damaging the connector. The recommended torque is 8 lbf-inch (100 N-cm). You could use a calibrated SMA torque wrench (for instance, from the Pasternack company, available at [www.pasternack.com](http://www.pasternack.com)).

Never leave the antenna connector without either the cap or the SMA connector. The antenna connector must be terminated to avoid damaging the device radio.

4. Apply two or three layers of electrical tape around all RF connections.  
The antenna cable and connectors are weather-tight; however, vibration caused by the wind will over time loosen the connectors and reduce the efficiency of the gaskets. The electrical tape will prevent this situation.
5. With SConfigurator, enter the new antenna gain and change the antenna selection from Integrated to External.
6. Carefully align the antenna with those of the other devices so that they have a clear RF line of sight.
7. To improve the signal level between both devices, use the antenna alignment utility from SConfigurator.

# 8

## Using the Web Interface

In addition to SConfigurator, another tool is available to interact with the device: the web interface. The web interface allows you to:

- View a quick status of the device
- Configure the device
- Perform maintenance operations

The web interface is only available with Microsoft Internet Explorer 6.0 or later. You may have to install or upgrade ActiveX controls when accessing the web interface for the first time or after updating your device from a previous firmware release.

Depending on user account and security settings, you may have to provide a user name and password when logging into the web interface or accessing it in secure mode. For more information, see the Security parameters on page 126.

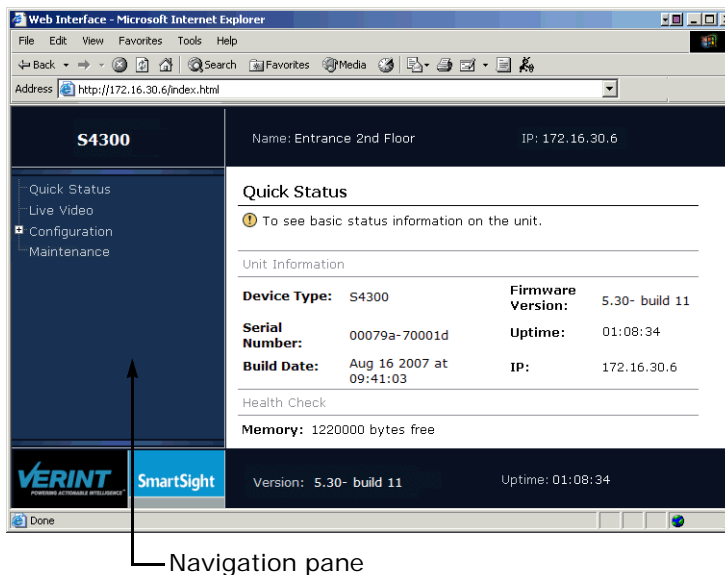


# Installing or Upgrading ActiveX Controls

The first time you access the web interface or after updating your device from a previous firmware release, you need to install or upgrade the ActiveX control for firmware update.

## To install or upgrade the ActiveX control:

1. Open a Microsoft Internet Explorer window.
2. Select **Tools > Pop-up Blocker > Turn Off Pop-up Blocker**.
3. If you upgraded the firmware of the device:
  - a. Select **Tools > Internet Options**.
  - b. In the **Temporary Internet files** box of the General tab, click **Delete Files**.
  - c. In the Delete Files window, check **Delete all offline content**, then click **OK**.
  - d. In the C:\Windows\Downloaded Program Files folder on your computer, delete the FwuEngineAx Class file.
4. In the **Address** box, enter the IP address of the device using the `http://IP_address` format.



5. Select **Tools > Internet Options > Security** to lower the security level in your web browser to enable the ActiveX component. Select **Trusted sites**, then click **Sites** to add the IP address of the device in the trusted sites list.
6. In the navigation pane, click **Maintenance**; then in the Maintenance pane, click **Update**. A yellow information bar appears below the Address box.

This site might require the following ActiveX control: 'FirmwareUpdateActiveX' from 'Verint Systems Canada Inc.'. Click here to install...

7. Click the information bar.
8. In the contextual window that appears, select **Install ActiveX Control**.
9. If your environment is Windows XP Service Pack 2 with Internet Explorer 6, click **Maintenance** in the navigation pane, then the **Update** button.
10. In the Internet Explorer - Security Warning window, click **Install**.



The ActiveX is installed.

11. Select **Tools > Pop-up Blocker > Turn On Pop-up Blocker**.

## Viewing the Quick Status

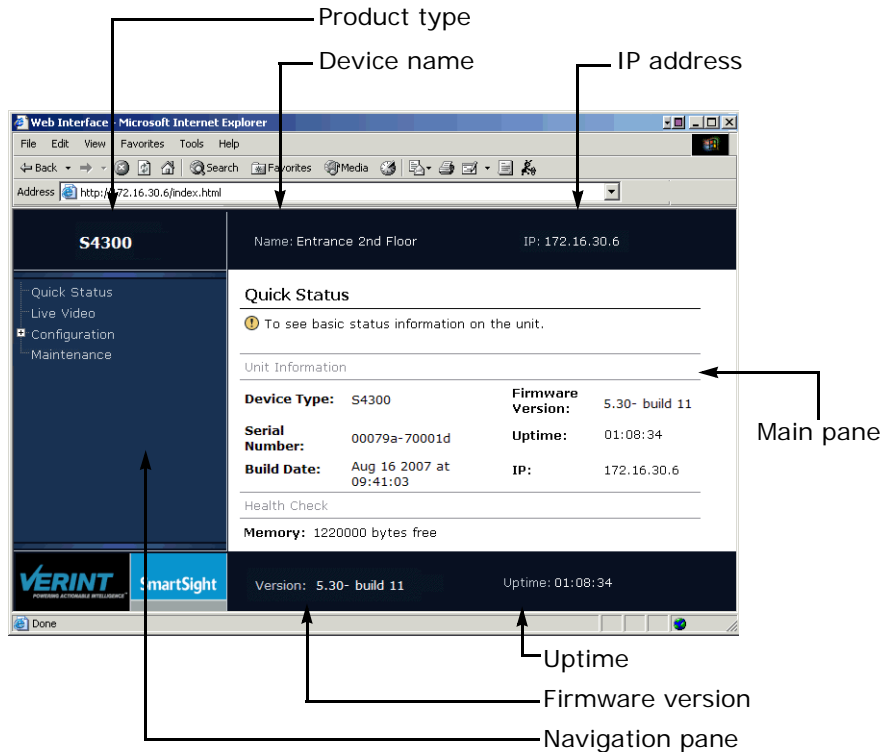
The Quick Status pane presents a summary of the device. It is the default view when you access the web interface. You may need to provide some of these internal parameters to customer service specialists for troubleshooting purposes. For a more complete view of internal parameters, look at the system status (described on page 128).

### To access the web interface:

1. Open a Microsoft Internet Explorer window.

## 8: Using the Web Interface

2. In the **Address** box, enter the IP address of the device using the `http://IP_address` format. The web interface window appears.

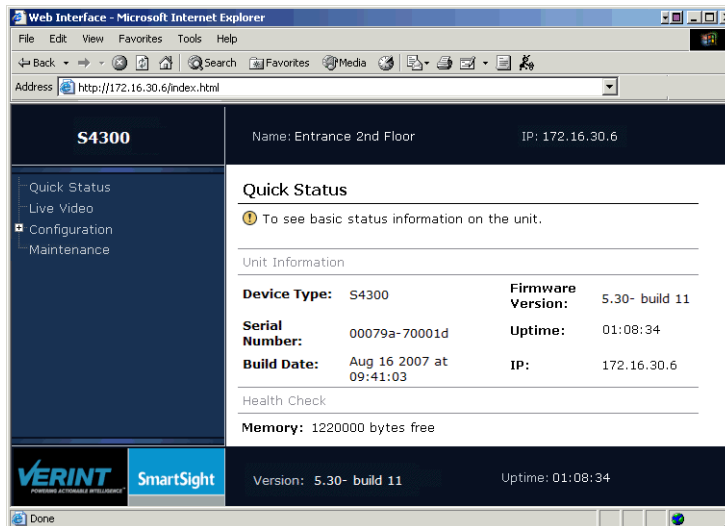


The web interface is composed of the following graphical elements:

- Product type—The type of the device.
- Device name—The descriptive name of the device. Go to page 135 to change it.
- IP address—The IP address of the device.
- Navigation pane—The types of information that are available in the web interface.
- Main pane—The area where to configure the device, view data, and perform maintenance tasks.
- Firmware version—The current firmware version of the main processor of the device. The latest firmware files are available on the Verint Video Intelligence Solutions extranet.
- Uptime—The time since the device has been rebooted, using the following format: *x days hh:mm:ss*; the “days” portion does not appear if the uptime is less than one day. The uptime is not automatically refreshed; press F5 to update it.

To view the quick status of the device:

1. In the navigation pane, click **Quick Status**. Basic information appear in the main pane.



The quick status information contains:

- ❑ Device Type—The type of the device. This information is also displayed on the top banner of the web interface.
- ❑ Serial Number—The serial number of the device.
- ❑ Build Date—The date the firmware has been generated.
- ❑ Firmware Version—The current firmware version of the device. This information is also displayed on the bottom banner of the web interface.
- ❑ Uptime—The time since the device has been rebooted. This information is also displayed on the bottom banner of the web interface.
- ❑ IP—The IP address of the device. This information is also displayed on the top banner of the web interface.
- ❑ Memory—The available internal memory in the device.

## Configuring the Device

The following parameter categories are available for configuration on the device:

- Access management
- Wireless communication
- System time
- System status
- VSIP
- HTTP (Webserver)
- Network

## Configuring Access Management

Access management takes care of user accounts and device security.

### User Accounts

You can protect the configuration of the device by restricting the access to its command line interface (CLI) and web interface with a user name and a password. You activate user accounts with the Use Telnet Accounts and Use Web Client Accounts parameters in the Security page (see page 126).

Two types of users are available:

- Administrator—Has all rights and is automatically available when user accounts are activated.
- Web client—Only has access to quick status in the web interface. Five web clients are available.

To configure the user accounts:

1. In the navigation pane, expand **Configuration > Access Management**, then click **User Accounts**. The user account parameters appear.

**S4300** Name: Entrance 2nd Floor IP: 172.16.30.6

**Device Configuration**

This page displays configuration information.

**User Accounts**

**Administrator User Name**  
User name should have between 4 and 40 characters and no space

**Administrator Password**  
Password should have between 4 and 40 characters and no space

**Web Client 1 User Name**

**Web Client 1 Password**

**Web Client 1**

**Web Client 2 User Name**

**Web Client 2 Password**

**VERINT** SmartSight Version: 5.30- build 11 Uptime: 01:08:34

2. In the **Administrator User Name** box, enter the alphanumeric string identifying the administrator user.
3. In the **Administrator Password** box, enter the alphanumeric string protecting the access to the device for the administrator user.
4. In the **Web Client x User Name** box, enter the alphanumeric string identifying a web client user.
5. In the **Web Client x Password** box, enter the alphanumeric string protecting the access to the device for a web client user.
6. In the **Web Client x** list, indicate whether the web client number x is enabled.

7. If required, repeat the web client configuration steps for all web client users. Up to five web clients are available.
8. To continue the configuration process, select another parameter category in the navigation pane. Otherwise, click **Apply** to save the changes in the device. Depending on the changes you made, a reboot may be required; follow the on-screen instructions in the Device Configuration Submittal pane.

## Security

The security parameters are relative to the protection of the device.

### To configure the security parameters:

1. In the navigation pane, expand **Configuration > Access Management**, then click **Security**. The security parameters appear.

S4300	
Name: Entrance 2nd Floor	IP: 172.16.30.6
<b>Device Configuration</b>	
This page displays configuration information.	
<b>Security</b>	
<b>Telnet Session</b>	Allow
<b>Use Telnet Accounts</b>	Disabled
<b>XML Report Generation</b>	Allow
<b>IP Firmware Update</b>	Allow
<b>HTTP Access</b>	Enabled
<b>HTTPS Access</b>	Enabled
<b>Use Web Client Accounts</b>	Disabled
<b>Global Security Profile</b>	Disabled
<b>SSL Passkey</b>	...
The passkey for SSL authentication (a maximum of 10 characters).	
Apply	

VERINT SmartSight Version: 5.30- build 11 Uptime: 01:08:34

2. In the **Telnet Session** list, indicate whether the access to the CLI of the device with Telnet is allowed.
3. In the **Use Telnet Accounts** list, indicate whether the use of user accounts to access the device with the CLI is enabled. To define user accounts, see page 125.
4. In the **XML Report Generation** list, indicate whether the generation of an XML report presenting the current state of the device is allowed.
5. In the **IP Firmware Update** list, indicate whether firmware updates on the device through the IP network are allowed.
6. In the **HTTP Access** list, indicate whether the access to the web interface of the device in a non-secure context is allowed. If you block this access, you can only set up the device with SConfigurator or Telnet.
7. In the **HTTPS Access** list, indicates whether the access to the web interface of the device in a secure HTTP (HTTPS) context is enabled.

8. In the **Use Web Client Accounts** list, indicate whether the use of user accounts to access the device with the web interface is enabled. To define user accounts, see page 125.
9. In the **Global Security Profile** list, indicate whether the complete SSL security on the device is enabled. Once this profile is activated on a device:
  - ☐ You cannot access it anymore with Telnet.
  - ☐ You cannot perform firmware updates through the IP network.
  - ☐ You access its web interface in a secure mode (that is, the HTTPS access mode is enabled).
10. In the **SSL Passkey** box, enter a password to secure the connection with the device. The passkey must be the same for all devices and the software tools to allow proper secure communication between them.

Tip: You should not change this passkey with the web interface, since there could be eavesdropping on the network. You can use SConfigurator or a video management software to change it.

11. To continue the configuration process, select another parameter category in the navigation pane. Otherwise, click **Apply** to save the changes in the device. Depending on the changes you made, a reboot may be required; follow the on-screen instructions in the Device Configuration Submittal pane.

## Viewing the System Status

The system status information indicates the current values of internal device parameters. These internal parameters are useful when troubleshooting the device with the assistance of a customer service specialist.

**To view the system status of the device:**

1. In the navigation pane, expand **Configuration**, then click **System Status**. The system status parameters appear.

S4300	
Name: Entrance 2nd Floor	IP: 172.16.30.6
<b>Device Configuration</b>	
This page displays configuration information.	
<b>System Status</b>	
Firmware Version	5.30- build 11
Loader Version	4.09- build 4
Booter Version	5.00- build 91
PIC Firmware Version	1.00- build 4
Build Date	Aug 16 2007 at 09:41:03
CPU Info	v4.0
CPU Frequency	351000000
Slave CPU Frequency	0
Slave Memory Size	0
Slave CPU Count	0
Uptime	01:08:34
Serial Number	00079a-700021
CPLD Version	0
Board Version	0
Internal Value 1	16000000 / 32
Audio Hardware	Absent
Unit Tested (MM-YY)	Not Available
Board Temperature	28 C

Verint SmartSight Version: 5.30- build 11 Uptime: 01:08:34

The following information is available:

- ❑ Firmware Version—The current firmware version of the main processor of the device. The latest firmware files are available on the Verint Video Intelligence Solutions extranet.
- ❑ Loader Version—The version of the firmware used to load the device.
- ❑ Booter Version—The version of the firmware used to boot the device.
- ❑ PIC Firmware Version—The version of the firmware used in the PIC (programmable intelligent controller) microcontroller.
- ❑ Build Date—The date the firmware has been generated.
- ❑ CPU Info—The version of the processing unit in the device.
- ❑ CPU Frequency—The frequency (in Hz) of the processing unit in the device.
- ❑ Slave CPU Frequency—The frequency (in Hz) of the slave processing unit in the device. A value of 0 indicates that there is no slave CPU in the device.
- ❑ Slave Memory Size—The size of the memory block in the slave processing unit, in bytes. A value of 0 indicates that there is no slave CPU in the device.



- ❑ Slave CPU Count—The number of slave processing units in the device.
- ❑ Uptime—The time since the device has been rebooted.
- ❑ Serial Number—The serial number of the device.
- ❑ CPLD Version—The version of the complex programmable logic device.
- ❑ Board Version—The version of the main board in the device.
- ❑ Internal Value 1—Verint technical information.
- ❑ Audio Hardware—The indication of whether audio hardware is present on the device.
- ❑ Unit Tested (MM-YY)—The date the device was tested by Verint production.
- ❑ Board Temperature—The temperature of the main board (in degrees Celcius).

## Configuring the Network

The network parameters allow communication between the device and its IP network. For more information about these settings, contact your network administrator.

**To configure the network parameters:**

1. In the navigation pane, expand **Configuration**, then click **Network**. The network parameters appear.

S4300	
Name: Entrance 2nd Floor	IP: 172.16.30.6
<b>Device Configuration</b> <i>This page displays configuration information.</i>	
<b>Network</b>	
<b>DHCP Configuration</b>	Disabled
<b>Local IP Address</b>	172.16.30.6
<b>Subnet Mask</b>	255.255.0.0
<b>Gateway</b>	169.254.0.6
<b>Host Name</b> <small>Enter host name (24 characters max)</small>	
Apply	
<b>VERINT</b> SmartSight Version: 5.30- build 11      Uptime: 01:08:34	

2. In the **DHCP Configuration** list, indicate whether DHCP (Dynamic Host Configuration Protocol) is used to automatically provide a valid network configuration for the device. You can set this option only if the device is connected to a network that uses a DHCP server. For more information about DHCP, see Appendix B on page 152.
3. In the **Local IP Address** box, enter the unique IP address of the device on the network. The IP address is written as four numbers separated by periods; each number is in the 0–255 range. Each device on a network must have a unique IP address.
4. In the **Subnet Mask** box, enter the binary configuration that specifies the subnet in which the IP address of the device belongs. A subnet is a portion of a network that shares a common address component. Unless otherwise specified by your network administrator, it is recommended to use a subnet mask of 255.255.0.0.

5. In the **Gateway** box, enter the IP address of the network point that acts as an entrance to another network. Never use the IP address of the device as the gateway value.
6. In the **Host Name** box, enter an alias for the IP address of the device, to be used by the DNS server; this parameter is optional. It is made up of 2 to 24 alphanumerical characters; the first one must be a character.

Note: It is up to the DHCP server to register the host name in the DNS server.

7. To continue the configuration process, select another parameter category in the navigation pane. Otherwise, click **Apply** to save the changes in the device. Depending on the changes you made, a reboot may be required; follow the on-screen instructions in the Device Configuration Submittal pane.

## Configuring Wireless Communication

The wireless communication parameters are relative to radio frequency (RF). There are two sets of parameters: basic and advanced.

### Basic Wireless

The basic parameters cover standard wireless features.

**To configure the basic wireless parameters:**

1. In the navigation pane, expand **Configuration**, then click **Wireless Communication**. The basic wireless communication parameters appear.

The screenshot shows the S4300 Device Configuration page. The left navigation pane has a tree view with 'Quick Status', 'Configuration', 'Access Management', 'System Status', 'Network', 'Wireless Communication' (highlighted), 'Advanced', and 'Maintenance'. The main content area is titled 'Device Configuration' and includes a warning icon and text: 'This page displays configuration information.' Below this is the 'Wireless Communication' section. It contains the following fields and values:

- MAC Mode:** SPCF (dropdown)
- Passkey:** Contains 16 characters or 32 hexadecimal digits. (text field with 16 dots)
- MAC Role:** Master (dropdown)
- RF Band:** Public Safety (4.9GHz OFDM) (dropdown)
- Channel:** Auto (dropdown)
- Channel Bandwidth:** 20 MHz (dropdown)
- Tx Bit Rate:** Auto (dropdown)
- Antenna Gain:** 11 dBi (text field)
- Antenna Selection:** Integrated (dropdown)
- Country:** UNITED\_STATES (dropdown)

At the bottom of the configuration section is an 'Apply' button and a message: 'Some parameters are automatically applied.' The footer of the page shows the Verint logo, 'SmartSight' branding, 'Version: 5.30- build 11', and 'Uptime: 01:08:34'.

2. In the **MAC Mode** list, select SPCF. The available media access control values are:
  - ❑ SPCF—The proprietary protocol that uses AES encryption (with key rotation) over the wireless link to secure communication between the devices and resolve “hidden node,” quality of service, range, and problems inherent to 802.11 wireless networking products.
  - ❑ SDCF—The legacy proprietary protocol not used anymore. It used AES encryption and resolved the range and security problems of the 802.11 standard, but did not manage the hidden node issue.
3. In the **Passkey** box, enter a unique user-supplied, case-sensitive identifier enabling secure and encrypted RF communication in the wireless cell. The passkey must have exactly 16 characters or 32 hexadecimal digits.

For the wireless connection to be secure, do not enter a known name (like a street name), but instead use a mix of digits and letters. Do not disclose the passkey. The connection security is based on the secrecy and uniqueness of the passkey. It is good practice to change the default passkey during the configuration process.

4. In the **MAC Role** list, select the function of the device in the wireless system. The available values are:
  - ❑ Master—A device that controls the access over the wireless medium. It takes care of channel selection and slave authentication to provide access to the wireless medium. The master also allocates bandwidth for all connected slaves.
  - ❑ Slave—A device that needs a master to access the wireless medium to transfer data. A slave can also bridge data.

**Note:** A change to the MAC role is automatically applied because it has an immediate impact on other parameters. However, this change will take effect in the device only after you save the parameter and reboot the S4300.

5. In the **RF Band** list, select the radio frequency band used by the device. The available values are:
  - ❑ 802.11a (5 GHz OFDM)
  - ❑ 802.11g (2.4 GHz OFDM)
  - ❑ Public Safety (4.9 GHz OFDM)

**Note:** A change to the RF band is automatically applied because it has an immediate impact on other parameters. However, this change will take effect in the device only after you save the parameter and reboot the S4300.

6. In the **Channel** list, select the frequency channel, within the selected band, that the wireless system will use. You can perform channel selection on master devices only; two selection methods are available: manual (selecting a specific channel) or automatic (with the Auto value). On a slave device, you can specify an initial value for the *roaming* process by which the S4300 will find its access point; be aware that this initial channel may not be the one used by the access point.

In a 4.9 GHz band context, the list of channels varies depending on the chosen bandwidth.

7. In the **Channel Bandwidth** list, select the width of the frequency channel when the 4.9 GHz public safety band is selected. This parameter only appears for the 4.9 GHz RF band. The values can be 5 MHz, 10 MHz, and 20 MHz (default).

Note: A change to the channel bandwidth is automatically applied because it has an immediate impact on other parameters. However, this change will take effect in the device only after you save the parameter and reboot the S4300.

8. In the **Tx Bit Rate** list, select the data rate at which the device operates. A high bit rate reduces the effective distance between two functional devices. You can set the bit rate in slave devices only.

When a slave connects to its master for the first time, it automatically receives the best possible value (the Auto value), with a default RF margin set to 15 dB (to change the margin, see page 134).

Once the device is operating properly, Verint strongly recommends to change the configured bit rate from Auto to the actual bit rate of the connection. This way, the wireless communication will be more stable in the presence of changing atmospheric conditions or other RF interferers. To know the actual bit rate of the connection, look in the Advanced > Communication Status and Statistics > Wireless Status menu of the CLI. If the quality of the RF link degrades severely, the actual bit rate could be lower than the manually configured one.

The available bit rates for the S4300 device are:

Band	Channel width	Bit rates (Mbps)
2.4 GHz	20 MHz	6, 9, 12, 18, 24, 36, 48, and 54
4.9 GHz	5 MHz	1.5, 2.25, 3, 4.5, 6, 9, 12, and 13.5
	10 MHz	3, 4.5, 6, 9, 12, 18, 24, and 27
	20 MHz	6, 9, 12, 18, 24, 36, 48, and 54
5 GHz	20 MHz	6, 9, 12, 18, 24, 36, 48, and 54

9. In the **Antenna Gain** box, enter the gain of the antenna on the device (in dBi).

You must enter the gain if you use an external antenna with your device; with this value, the device will be able to automatically change its transmission power so that the total power (device and antenna) does not exceed the maximum value established by your country's regulations.

With the integrated antenna, you should also validate that the proper value for the selected RF band is displayed; the gain is 8.5 dBi in the 2.4 GHz band and 12 dBi in the 4.9 GHz and 5 GHz bands.

Note: Providing a gain lower than the gain of the antenna used by the device is strictly prohibited.

10. In the **Antenna Selection** list, select the type of antenna that will be used on the device. The available values are:
  - ☐ Integrated—To use the tri-band antenna coming with the device.
  - ☐ External—If you installed a high gain antenna.
11. In the **Country** list, select the proper country of operation to the device, to comply to the DFS/TPC regulations if applicable, to respect the maximum EIRP, and to use the proper set of frequency channels.
12. To continue the configuration process, select another parameter category in the navigation pane. Otherwise, click **Apply** to save the changes in the device. Depending on the changes you made, a reboot may be required; follow the on-screen instructions in the Device Configuration Submittal pane.

## Advanced Wireless

The advanced parameters provide more elaborate features.

To configure the advanced wireless parameters:

1. In the navigation pane, expand **Configuration > Wireless Communication**, then click **Advanced Wireless**. The advanced wireless communication parameters appear.

The screenshot displays the Verint SmartSight web interface. On the left is a navigation pane with a tree structure: Quick Status, Configuration (expanded), Access Management, System Status, Network, Wireless Communication (expanded), Advanced Wireless (selected), Advanced, and Maintenance. The main content area is titled 'Device Configuration' and includes a warning icon and text: 'This page displays configuration information.' Below this is the 'Advanced Wireless' section with the following settings:

- Passkey Entry Format:** String (dropdown)
- Tx Power Scale:** Maximum (dropdown)
- Sensitivity Threshold:** Normal (dropdown)
- Starting Order:** 1 (dropdown)
- Minimum Margin:** 15 (text input) dB  
*Possible choices: 0 to 50 dB*
- Enable Radar Detection On Slave:** Disabled (dropdown)
- Number of Frames per Burst:** 8 (text input)  
*1-8*
- Maximum Polling Latency:** 255 (text input) ms  
*10-255 [255]=No Latency Control*
- IP Multicast Forward from this Interface:** Allowed (dropdown)
- Indoor/Outdoor RF Regulation:** Indoor/Outdoor (dropdown)
- DFS/TPC Adjacent Channel Removal:** Enabled (dropdown)

An 'Apply' button is located at the bottom of the configuration section. The footer of the interface shows the Verint SmartSight logo, the version '5.30- build 11', and the uptime '01:08:34'.

2. In the **Passkey Entry Format** list, select the format for the wireless and WEP passkeys. The available values are String and Hexadecimal.

3. In the **Tx Power Scale** list, select the level of emitting power of the device radio. The default level is the maximum allowed in your country for the configured antenna. If your system operates with a comfortable RF margin (15 dB), you may reduce the emitting power to lower the noise generated on the other RF systems located nearby. The available values are:
  - ☐ Maximum—The maximum allowed.
  - ☐ 50%—The power is reduced by 3 dB.
  - ☐ 25%—The power is reduced by 6 dB.
  - ☐ 12.5%—The power is reduced by 9 dB.
4. In the **Sensitivity Threshold** list, select the minimum signal level perceived by the radio of the device. Reducing the sensitivity of the radio enables unwanted “noise” to be filtered out. A safe value is 10 dB below the current received signal level (displayed in the CLI in the Advanced > Communication Status and Statistics > Wireless Status menu). The default value, Normal, represents the most sensitive context. You must be careful not to reduce the sensitivity to a level where the device would not “hear” its legitimate correspondent. The other available values are -80 dBm, -75 dBm, -70 dBm, and -60 dBm.
5. In the **Starting Order** list, select the sequence number, used during the boot-up process of a master device in a DFS context with automatic frequency channel selection, to delay its startup. The purpose of this parameter is to ensure that colocated master devices will not start at the same time. The default starting order is 1. Every colocated cell should have a different starting order: It should be incremented by 1 in each system. This parameter is not used if channel selection is manual.
6. In the **Minimum Margin** box, enter the difference in dB between the actual signal received by the device and the minimum signal required by a given bit rate to correctly receive data on the RF link. The default minimum margin is 15 dB. This parameter is used when the transmission bit rate is set to Auto.
7. In the **Enable Radar Detection on Slave** list, indicate whether radar detection is enabled on slave devices in a DFS context; this parameter only appears if the selected RF band supports DFS. For more information on radar detection, see page 33.
8. In the **Number of Frames per Burst** box, enter the maximum number of data frames that are sent on the wireless network by a slave device each time its master polls it. The value range is 1–8. Default is 8. The performance of the wireless network increases as the number of frames increases.
 

Typically this value is set on a slave device to configure its connection to its master. Setting this value on the master limits the maximum number of frames for all slaves connected to it. If a slave has a lower limit than the value provided by the master, the lowest limit will be taken.
9. In the **Maximum Polling Latency** box, enter the maximum delay between two polls for the same slave, in milliseconds. The value range is 10–255. Default is 255: It indicates that there is no latency control and provides the maximum performances.
 

SPCF is a polling protocol. Each slave is polled one after the other. The polling latency is the time taken to poll all the connected slaves. For delay sensitive applications like PTZ, it can be useful to have control on this delay. When enabled, polling latency control will automatically adjust the maximum number of frames per burst for each slave so that the maximum latency delay is respected. However, doing so reduces the maximum performances of the wireless network.

10. In the **IP Multicast Forward from this Interface** list, indicate whether multicast data coming from the wireless network is allowed to be sent to the Ethernet network.
11. In the **Indoor/Outdoor RF Regulation** list, select the regulation regarding the location of the device; the location depends on the country of operation and frequency band. The available values are Indoor, Outdoor, or Indoor/Outdoor. The available frequency channels are different for each location regulation. The default factory value for most countries is Indoor/Outdoor.  
  
Under the RF regulation, a device programmed to be used only indoors must not be installed outdoors, and vice versa.  
  
To know which frequency channels are available in your country of operation in each of the three operation modes, see the "Compliance" appendix on page 183.
12. In the **DFS/TPC Adjacent Channel Removal** list, indicate whether the available list of frequency channels is reduced to avoid the use of adjacent channels. For more information, see page 33.
13. To continue the configuration process, select another parameter category in the navigation pane. Otherwise, click **Apply** to save the changes in the device. Depending on the changes you made, a reboot may be required; follow the on-screen instructions in the Device Configuration Submittal pane.

## Configuring VSIP

Parameters are available to configure the VSIP proprietary communication protocol.

### To configure the VSIP parameters:

1. In the navigation pane, expand **Configuration > Advanced**, then click **VSIP**. The VSIP parameters appear.

S4300	Name: Entrance 2nd Floor	IP: 172.16.30.6
<ul style="list-style-type: none"> <li>Quick Status</li> <li>Configuration               <ul style="list-style-type: none"> <li>Access Management</li> <li>System Status</li> <li>Network</li> <li>Wireless Communication</li> <li>Advanced                   <ul style="list-style-type: none"> <li><b>VSIP</b></li> <li>System Time</li> <li>HTTP (Webserver)</li> </ul> </li> <li>Maintenance</li> </ul> </li> </ul>	<h3>Device Configuration</h3> <p> This page displays configuration information.</p> <hr/> <h4>VSIP</h4> <p><b>VSIP Port</b> The VSIP communication port of the unit. IP ports 9541, 65500, and those under 1028 must not be used.</p> <p><input type="text" value="24824"/></p> <p><b>VSIP Multicast IP Address</b> The multicast IP address used by the unit to listen for VSIP queries.</p> <p><input type="text" value="224.16.32.1"/></p> <p><b>VSIP Discovery IP Address</b> The IP address used by the unit to make its presence known on the network.</p> <p><input type="text" value="255.255.255.255"/></p> <p><b>VSIP Unit Name</b> The name of the unit.</p> <p><input type="text" value="Entrance 2nd Floor"/></p> <p><input type="button" value="Apply"/></p>	
	Version: 5.30- build 11	Uptime: 01:08:34

2. In the **VSIP Port** box, enter the communication port used by the device. The default value of all Nextiva devices is 5510.

Note: VSIP ports 9541, 65500, and those under 1024 are reserved and should not be used, not even for serial port, video, or audio communication. The maximum value is 65535.

3. In the **VSIP Multicast IP Address** box, enter the IP address used by the device to listen for VSIP queries. The current multicast address is 224.16.32.1 and should not be changed.
4. In the **VSIP Discovery IP Address** box, enter the IP address used by the device to make its presence known with the broadcast method. The broadcast address is 255.255.255.255.
5. In the **VSIP Unit Name** box, enter the name of the device, as displayed in the top of the web interface and in the first column of the SConfigurator unit list.
6. To continue the configuration process, select another parameter category in the navigation pane. Otherwise, click **Apply** to save the changes in the device. Depending on the changes you made, a reboot may be required; follow the on-screen instructions in the Device Configuration Submittal pane.

## Configuring System Time

The device can connect to a Network Time Protocol (NTP) server to get the current time. The main reason to use NTP is to display valid dates in the log files instead of the device uptime.

The Local Time parameter indicates the current local time if the device is connected to an NTP server.



**To configure the system time parameters:**

1. In the navigation pane, expand **Configuration > Advanced**, then click **System Time**. The system time parameters appear.

The screenshot shows the Verint SmartSight web interface. On the left is a navigation pane with a tree structure: Quick Status, Configuration (expanded), Access Management, System Status, Network, Wireless Communication, Advanced (expanded), VSIP, **System Time** (selected), HTTP (Webserver), and Maintenance. The main content area is titled 'Device Configuration' for device 'S4300' (Name: Entrance 2nd Floor, IP: 172.16.30.6). It includes a note: 'This page displays configuration information.' Below this is the 'System Time' section with the following fields: 'NTP Server Usage' (a dropdown menu set to 'Disabled'), 'NTP Server IP Address' (a text box with '0.0.0.0' and a description: 'The IP address of the NTP server from which the unit will get the current time.'), 'NTP Server IP Port' (a text box with '123' and a description: 'The IP port of the NTP server. Standard value is 123.'), 'Local Time Offset' (a text box with '0' and a description: 'The offset from the GMT time in the current time zone (e.g., EST = -300 minutes).'), and 'Local Time' (a text box with 'No valid date has been registered.'). An 'Apply' button is at the bottom of the configuration section. The footer shows the Verint logo, SmartSight logo, Version: 5.30- build 11, and Uptime: 01:08:34.

2. In the **NTP Server Usage** list, indicate whether Network Time Protocol (NTP) is used to get the current time. NTP uses GMT to synchronize device clock time.
3. In the **NTP Server IP Address** box, enter the IP address of the NTP server from which the device will get the current time.
4. In the **NTP Server IP Port** box, enter the IP port of the NTP server. Default is 123.
5. In the **Local Time Offset** box, enter the offset in minutes from the GMT time in the time zone in which the device operates (for instance, the offset for the Eastern Standard Time is -300 minutes).
6. To continue the configuration process, select another parameter category in the navigation pane. Otherwise, click **Apply** to save the changes in the device. Depending on the changes you made, a reboot may be required; follow the on-screen instructions in the Device Configuration Submittal pane.

## Configuring HTTP (Webserver)

A series of parameters help configure the communication between the web page on the computer and the device.

**To configure the HTTP parameters:**

1. In the navigation pane, expand **Configuration > Advanced**, then click **HTTP (Webserver)**. The HTTP parameters appear.

**Note:** If you change any of these parameters, you must refresh the web page (for instance, by pressing F5).

The screenshot shows the S4300 device configuration interface. The left navigation pane is expanded to 'Configuration > Advanced > HTTP (Webserver)'. The main content area is titled 'Device Configuration' and contains the following settings:

- HTTP (Webserver)** section:
  - HTTP Server IP Port:** A text box containing '80'. Below it, a note states: 'The default port number for this server is 80.'
  - WEB Streaming Method:** A dropdown menu with 'VSIP/TCP' selected.
  - Apply** button.

At the bottom of the page, the Verint SmartSight logo is visible, along with the version '5.30- build 11' and uptime '01:08:34'.

2. In the **HTTP Server IP Port** box, enter the TCP port number in the device on which the HTTP requests will be made. Default in all web applications is 80.
3. In the **Web Streaming Method** list, select the protocol used for transmitting video. The available values are:
  - ❑ VSIP/UDP—A legacy protocol, using the proprietary VSIP video protocol over UDP. The preferred UDP mode is RTP/UDP.
  - ❑ VSIP/TCP—A protocol using the proprietary VSIP video protocol over TCP. This protocol guarantees proper reception of video packets, but could slow down the effective frame rate to an unacceptable level (default).
  - ❑ Multicast UDP—A protocol using RTP (Real Time Transport Protocol, RFC 3550) over UDP that transfers video to a multicast group. It does not guarantee proper reception of video packets.
  - ❑ RTP/UDP—A protocol using RTP (Real Time Transport Protocol, RFC 3550) over UDP that transfers video to a unique recipient. It does not guarantee proper reception of video packets.
4. To continue the configuration process, select another parameter category in the navigation pane. Otherwise, click **Apply** to save the changes in the device. Depending on the changes you made, a reboot may be required; follow the on-screen instructions in the Device Configuration Submittal pane.

# Maintaining the Device

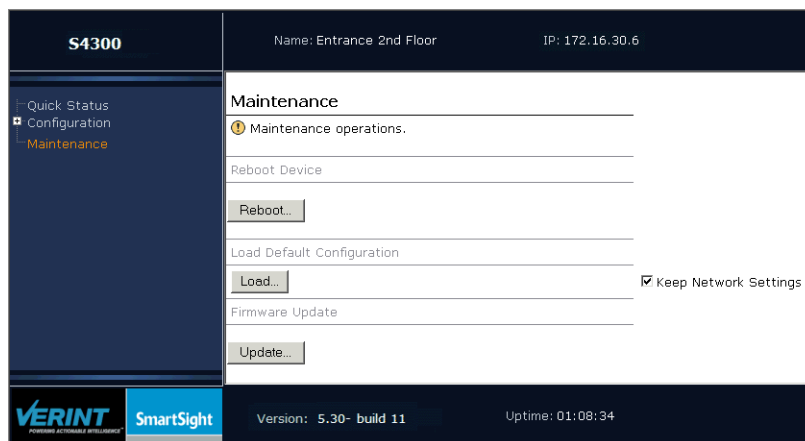
The following maintenance tasks are available on the web interface:

- **Reboot**—To restart the device, while keeping its current configuration and saving the changes.
- **Load**—To assign the factory default settings to the device. You may keep the values of many network parameters. The default values are listed in Appendix A on page 150.
- **Update**—To upgrade the firmware of the device.

For more information about these tasks and when you should perform them, see the “Maintaining and Troubleshooting the Device” chapter.

## To reboot the device:

1. In the navigation pane, click **Maintenance**. The maintenance pane appears.



2. Click **Reboot**. A confirmation window appears.
3. Click **OK**.

## To load the default values of the device:

1. In the navigation pane, click **Maintenance**. The maintenance pane appears.
2. To keep the following network parameters, ensure that **Keep Network Settings** is checked:

- DHCP usage    ■ Gateway    ■ Ping request target    ■ Subnet
- IP address    ■ DNS servers    ■ Ping request size    ■ Host name

Otherwise, you will need to reprogram the device for proper operation within the network.

3. Click **Load**. A confirmation window appears.

4. Click **OK**. The default values are applied.

#### To update the firmware of the device:

**Note:** If you upgraded the device firmware or are accessing the firmware update process for the first time, you need to install an ActiveX prior to proceeding (for more information, see page 121).

1. In the navigation pane, click **Maintenance**. The maintenance pane appears.
2. Click **Update**. The Firmware Update page appears.

3. In the Firmware File group box, click **Browse**.
4. In the Open dialog box, select the firmware file to use, then click **Open**.
5. Click **Start**.

The upgrade operation is executed.

If the update procedure fails:

1. Restart the same procedure immediately.
2. If the problem persists, reboot the device, then restart the update procedure.
3. If the problem persists, connect an Ethernet cable between the device and the network used by the host computer; then start again the update procedure.
4. If the problem persists, look at the status LEDs for abnormal behavior.

You should take into consideration the following facts regarding firmware updates using the IP network:

- It can be deactivated in the command line interface (CLI) or the web interface.

- Ensure that the IP link is stable before starting the procedure; therefore it is not recommended to perform it over the Internet.

# 9

## Maintaining and Troubleshooting the Device

There are many ways to update the firmware of the device.

Also, you may need to troubleshoot the device:

- Detecting a duplicate master
- Finding a lost device
- Performing a reset
- Recognizing the status LED conditions
- Using the command line interface
- Selecting a frequency channel

## Updating the Firmware

You may need to update the S4300 to have access to new firmware or new features. Updating the firmware of a device retains its configuration. Many tools are available to perform the update: the SConfigurator utility, the web interface (see page 140), or a video management software like Verint Nextiva; for the detailed procedure, refer to the documentation of the software.

The latest firmware files are available on the Verint Video Intelligence Solutions extranet (Quick Links > Firmware and Applications > Nextiva Intelligent Edge Devices).

Note: Firmware downgrade is not supported on any device. If you perform a downgrade, any problem encountered will not be covered by your product warranty.

## Detecting a Duplicate Master

The duplicate master detection problem occurs when two S4300 master devices are using the same frequency channel and are seeing each other.

More specifically, the problem is detected when the second S4300 is booting up. This device refuses to start its wireless operations (to prevent any interference with the working setup) and makes its three LEDs flash red (1-second intervals). In the CLI of the device, the Current SPCF Connection Status parameter turns to Duplicate master detected (accessed through Advanced > Communication Status and Statistics > Wireless Status). Furthermore, an error message is logged in the device.

The already running master will not change its behavior. You must change the frequency channel of the second master.

## Finding a “Lost” S4300

The only way to access a device is through an Ethernet or wireless connection. You may have difficulty accessing it if you do not remember its IP address or VSIP port. For instance, if you enabled security on the device, you cannot access it with Telnet; if you lost its VSIP port, you cannot locate it with SConfigurator.

To find a “lost” S4300 device, use SConfigurator and the common VSIP port.

### To find a lost S4300:

1. Open SConfigurator.
2. In the General tab, click **Program Options**.
3. Click **Common** to set the common VSIP port, then click **OK**.
4. Click the **Units** tab.
5. Click **Discover**.

All devices on the network, regardless of their configurable VSIP ports, appear in the Units list. Locate the lost S4300 and write down its VSIP port and IP address in a safe place.

6. Click the **General** tab, then click **Program Options**.
7. In the **VSIP Port** box, enter the discovered value.

## Performing a Reset

Depending on the gravity of the situation, you can reboot the device or load its default configuration if the device does not react the way it should:

1. Start by rebooting the device. The device will retain all its configuration.
2. If it continues to perform abnormally, load its default configuration. All user-defined values will be lost.

### To reboot the device:

1. Perform one of the following operations:
  - In SConfigurator, go to the **Units** tab, select the device to reboot, click **Configure**, select the **Unit** entry in the parameter tree, then click **Reboot Unit**.
  - In the web interface, click **Maintenance** in the navigation pane, then click **Reboot**.

The device reboots, while retaining its configuration.

### To load the default configuration:

1. Perform one of the following operations:
  - In SConfigurator, go to the **Units** tab, select the device to reboot, click **Configure**, select the **Unit** entry in the parameter tree, then click **Load Default Settings**.
  - In the web interface, click **Maintenance** in the navigation pane. To keep the network configuration, check **Keep Network Settings**. Click **Load**.

This operation assigns the factory default settings to the device (listed in Appendix A on page 150). Following such a reset, you may need to reprogram the device (for instance, its IP address and VSIP port) for proper operation within its network.

## Recognizing the LED Conditions

The S4300 device comes with three bicolor (green-red) LEDs that provide detailed information on the device activity. Each LED can go through three phases:

1. Warmup period if the internal temperature is too low
2. Bootup
3. Normal operation



The three LEDs are:

- LAN—For the Ethernet network (802.3) status:

Condition	Indication
<b>Warmup</b>	
Red blinks (2.0 sec. intervals)	The internal temperature of the device is too low.
<b>Bootup</b>	
Steady red (10 sec.)	
Steady green (4 sec.)	
<b>Normal operation</b>	
Steady green	The device is connected to the Ethernet network.
Flashing green (1-sec. flash every 3 sec.)	The device is in normal operation but is not connected to the network.
Flashing green (0.1 sec. off for each packet)	A packet is received or transmitted.
Red blink (0.1 sec.)	There is a communication error.
Flashing red (0.1 sec. intervals)	The device is being identified.
Flashing red (1 sec. intervals) happening simultaneously on all LEDs	On a master device: There is another master currently running on the same frequency channel; for more information, see page 147.

- RF—For the wireless LAN (802.11) status:

Condition	Indication
<b>Warmup</b>	
Red blinks (2.0 sec. intervals)	The internal temperature of the device is too low.
<b>Bootup</b>	
Steady red (14 sec.)	
<b>Normal operation</b>	
Flashing green (1-sec. flash every 3 sec.)	The device is in normal operation without an RF connection.

Condition	Indication
Steady green	The device is in normal operation with at least one RF connection.
Flashing green (0.1 sec. off for each packet)	A packet is received or transmitted.
Red blink (0.1 sec.)	There is a communication error.
Flashing red (0.1 sec. intervals)	The device is being identified.
Flashing red (1 sec. intervals) happening simultaneously on all LEDs	On a master device: There is another master currently running on the same frequency channel; for more information, see page 147.

- System status—For the general device status:

Condition	Indication
<b>Warmup</b>	
Red blinks (2.0 sec. intervals)	The internal temperature of the device is too low.
<b>Bootup</b>	
Steady red (14 sec.)	
<b>Normal operation</b>	
Flashing green (1 sec. intervals)	The device is in normal operation.
Flashing red (1 sec. intervals)	<p>The IP address of the device is already assigned to another device on the network.</p> <p>or</p> <p>On a master device: There is another master currently running on the same frequency channel; for more information, see page 147. This condition happens simultaneously on all LEDs.</p>
Flashing green-red (1 sec. intervals)	The device is undergoing a firmware update.

Condition	Indication
Flashing red (0.1 sec. intervals)	The device is being identified.
Yellow blink (1 sec. intervals)	On a master device: The master is scanning for a channel in a DFS context.

The following power-up conditions on the three status LEDs are abnormal:

- LED not lit—Check the power supply and cabling. If power is available and the LED stays off, call Verint Video Intelligence Solutions technical support for assistance.
- Steady red or green LED for more than 30 seconds—There is an internal error that prevents the device from starting normally. Power down the device, wait 30 seconds, then power it up. If the condition persists, call Verint Video Intelligence Solutions technical support.

## Using the Command Line Interface

You may need to access the command line interface (CLI) of an edge device to perform troubleshooting tasks, typically with the assistance of a Verint customer service specialist.

The available troubleshooting tasks include configuring quality of service (QoS).

## Accessing the CLI

SConfigurator provides a network access to the CLI through the Telnet utility.

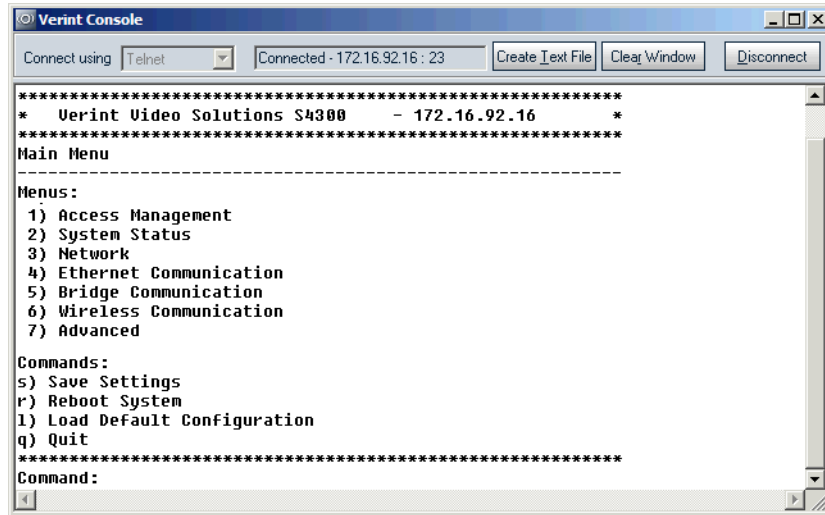
### To enter the CLI with Telnet:

Note: Ensure that your computer and the S4300 device are in the same IP subnet.

1. Open SConfigurator.
2. Click the **Units** tab.
3. Click **Discover**.

4. Select the desired device, then click **Telnet**.

The CLI main menu appears in the Verint Console window.



The CLI has a timeout that is triggered after three minutes of inactivity. When the timeout occurs:

- ☐ You lose access to the command line.
  - ☐ The "Thank you for using the Verint CLI" message appears at the command line.
  - ☐ The Verint Console window becomes disabled.
  - ☐ The Disconnect button switches to Connect.
5. To reactivate the CLI after a timeout, click **Connect**.
  6. To work through the CLI menu structure, follow these guidelines:
    - ☐ To execute a command or open a menu, type in the corresponding letter or number, then press **Enter**.
    - ☐ To return to the previous menu, enter **p**.
  7. To end the CLI work session:
    - a. Save the settings by entering **s** at the main menu, then pressing **Enter**.
    - b. Exit the CLI by entering **q** at the main menu, then pressing **Enter**.  
Depending on the changed settings, the device may perform a soft boot.
    - c. Close the Verint Console window.

**Note:** Do not use the Disconnect button to exit the CLI, since it does not save your settings.

## Configuring Quality of Service

Quality of Service (QoS) is a set of low-level networking protocols giving higher priority to more important data flows while ensuring that the less important ones do not fail. QoS is an essential technology for organizations rolling out a new generation of network applications such as real-time voice communications and high-quality video delivery.

In the Nextiva edge devices, the two available QoS flavors are Type of Service (ToS) and Differentiated Service Code Points (DSCP).

For QoS to be taken into account, the network infrastructure equipment (switches and routers) must support one of these protocols. If any of these devices does not support QoS, the QoS data will simply be processed as traditional non-QoS data. Furthermore, all Nextiva edge devices on a network must support the same QoS protocol (or no protocols at all).

You can set a priority flag to three data types coming out of an edge device: video, audio, and control. A QoS-enabled switch (or router) uses this flag to determine how the current data compares to what is currently going through it.

The QoS values are in the Advanced > Quality of Service menu.

## Selecting a Frequency Channel

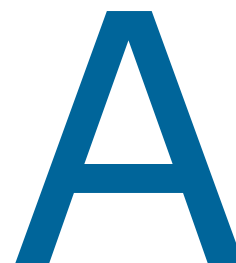
In large scale wireless systems, you should not use automatic channel selection. This mechanism uses a Verint best-effort algorithm that tries to avoid channel interferences. In large systems with colocated cells, the best way is to perform manual wireless planning. Verint offers system planning assistance; contact the customer service team for more information.

To help you select the appropriate frequency channels, perform a site survey on each device once your system is installed in its final location to detect potential interference problems. For the detailed procedure, see page 163.

Since the site survey available in the devices covers digital signals only, you should consider performing also an analog site survey with a spectrum analyzer, to detect potential radio or satellite signals.

The suggested procedure is:

1. Select the number of site survey iterations to perform.
2. Execute a site survey on each device in the wireless cell, one at the time, while the others are working. It is important to “hear” the signals coming from the other devices in the wireless cell.
3. Perform an analog site survey with a spectrum analyzer.
4. Analyze the data and change the frequency channel if required.



# **Factory Default Configuration**

The S4300 is programmed at the factory with the following configuration:

Type	Configuration
Access management	<ul style="list-style-type: none"> <li>■ User name: USERNAME</li> <li>■ Password: PASSWORD</li> <li>■ User accounts: Disabled</li> <li>■ Telnet sessions: Enabled</li> <li>■ IP firmware update: Enabled</li> <li>■ Global security profile: Disabled</li> <li>■ SSL passkey: &lt;empty&gt;</li> </ul>
Network	<ul style="list-style-type: none"> <li>■ DHCP configuration: Disabled</li> <li>■ IP address: 169.254.*.* (based on the MAC address of the device)</li> <li>■ Subnet mask: 255.255.0.0</li> <li>■ Gateway: 0.0.0.0</li> </ul>
Wireless Communication	<ul style="list-style-type: none"> <li>■ Wireless passkey: ABCDEFGHIJKLMNOP</li> <li>■ Channel: Auto</li> <li>■ Tx bit rate: Auto</li> <li>■ Antenna gain: 12 dBi</li> <li>■ Tx power scale: Maximum</li> </ul> <p>The frequency band and country vary depending of the purchased product.</p>
VSIP	<ul style="list-style-type: none"> <li>■ VSIP Port: 5510</li> <li>■ VSIP multicast IP address: 224.16.32.1</li> <li>■ VSIP discovery IP address: 255.255.255.255</li> </ul>



# DHCP Support and APIPA

DHCP (Dynamic Host Configuration Protocol) allows devices and computers connected to a network to automatically get a valid IP configuration from a dedicated server.

The APIPA (Automatic Private IP Addressing) scheme, available on the Windows operating systems, enables a device to assign itself a temporary IP address.



At startup, an edge device searches for a valid IP network configuration. The device requires this configuration prior to starting its functions. The network configuration for Nextiva devices consists of:

- An IP address
- A subnet mask
- A gateway

The device first looks in its local memory. If no configuration is found, it tries to contact a DHCP server. If DHCP configuration fails—if the device does not find a server or if it cannot get a configuration from it within one minute—the device assigns itself temporary network parameters based on the APIPA addressing scheme. This scheme allows a device to find a unique IP address until it receives a complete network configuration, either manually or from a DHCP server.

A device in APIPA mode does not reside on the same subnet as the other devices on the IP network; therefore, it may not be able to see or be visible by the other devices. Devices use the following temporary APIPA configuration:

- IP address: 169.254.X.Y (where *X* and *Y* are based on the last two digits of the MAC address of the device)
- Subnet mask: 255.255.0.0
- Gateway: 169.254. \*. \*

A device is in APIPA mode:

- The first time it boots up
- After receiving a duplicate IP address
- After a hardware reset
- When the DHCP server does not have any available IP addresses
- After loading the default parameters

DHCP configuration is automatically disabled after a factory reset.



# Surge Protection

Voltage and current surges can be induced by lightning strikes or power line transients. In the real world, under the right circumstances, these surges can reach sufficiently high levels to damage almost any electronic equipment. Therefore protection may be required on the following device ports:

- 12V/24V power
- External antenna
- Ethernet

For the curious mind, a surge protector helps to clamp the surge to safe levels and divert its energy to the earthing point, preventing device damage. Experienced installers know that an effective surge protection must be installed with proper earthing and grounding.

Visit the following sites to find interesting information about the statistical occurrences of lightning in your region (worldwide coverage):

- <http://earthobservatory.nasa.gov>
- <http://thunder.nsstc.nasa.gov/>

Excellent international sources for external surge protection equipment and general surge and lightning protection information are:

- Polyphaser Corporation—[www.polyphaser.com](http://www.polyphaser.com)
- Citel inc.—[www.citelprotection.com](http://www.citelprotection.com)
- Transtector—[www.transtector.com](http://www.transtector.com)

## 12V/24V Power

The S4300 provides a strong and complete form of surge protection on its 12V/24V power port. No additional protection is required.

However, if you are installing the equipment in a lightning prone or heavy lightning environment, or in a site where large AC mains power fluctuations are a common occurrence, you may need to add external surge protection to your power supply devices. For example, if the power feed of an S4300 runs down the pole or wall for more than 20 feet (7.6 meters), it is a good candidate for additional protection in a surge prone environment.

## External Antenna

The external antenna connector on the S4300 does not have surge protection; this situation should not cause problems as long as you keep the antenna cable short—that is, below 6.6 feet (2 meters).

## Ethernet Port

The basic CE-compliant form of protection implemented on the Ethernet port of the S4300 may not be sufficient to guarantee the product integrity under severe indirect lighting induction. Therefore you should add external surge protection modules for devices installed on a pole or tower, either on the ground or on a roof, to protect the Ethernet connection. Verint recommends to add an external protection module at each end of the Ethernet cable.

Verint does not provide any recommendation regarding the installation of external protection in cases not involving the mounting of the wireless device in an elevated position; for example, the mounting of the product against a building wall that naturally provides a more limited lightning exposure.

The surge protection module should be located within 1 meter of cable of the equipment. However, if the Ethernet equipment at the other end of the connection is inside a building, it is also acceptable to put the protector for this end at the entry point of the cable in the building. Here are typical examples:

- In a point-to-multipoint application, an S4300 is mounted on a pole in a parking lot; the pole is at 25 meters of the building, with the Ethernet cable being buried in the ground and going to an Ethernet switch in the building (the switch can have integrated PoE injection, external PoE injector, or 12/24V powering without PoE). It is highly probable that the pole will develop a high potential with regards to the grounding network of the building when the surge occurs, a situation even aggravated if the pole is poorly grounded (no grounding rods or mesh, dry soil, and so on).
- An S4300 in a wireless bridge application is mounted on a pole in a parking lot; the Ethernet cable travels down the pole and goes to an automatic gate system (with 12V or 24V power) at the base of the pole or close to it. Even if the pole may seem to be a good equi-potential conductor for the whole system (even if the pole is poorly grounded), it may not act as such if a severe lightning surge occurs. The peak current of a severe surge can develop thousands of volts between the top and bottom of the pole by inductive effect. This high potential can break the usual isolation of Ethernet devices to ground and permanently damage the equipments.

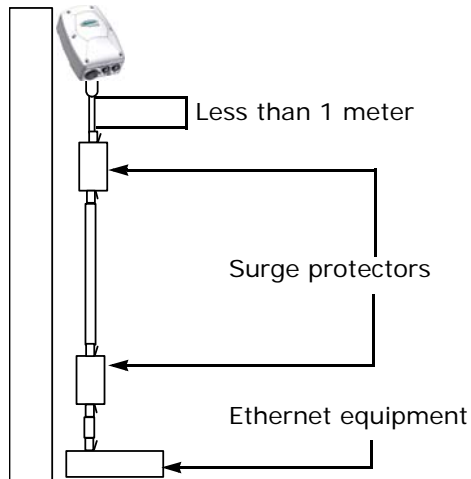
Verint has evaluated and tested two models of surge protection modules. Each one has its own characteristics and specific advantages, depending on the particular installation case:

Manufacturer	Model	Characteristics
Polyphaser	NX4-60	Non-waterproof enclosure (connectors) Extended temperature (outdoor) High surge level: <ul style="list-style-type: none"> <li>■ 3kA (8x60us)</li> <li>■ 300A (10x1000us)</li> </ul>
Transtector	ALPU-POE-60	Weatherproof enclosure (non-sealed design, bottom cable entries) Extended temperature (outdoor) Standard secondary protection surge level (reference GR-1089): 100A (10x1000us)

Verint recommends using the Transtector ALPU-POE-60 model for most installations in light to moderate lightning activity areas if the S4300 is mounted on a pole or tower. This surge protector being readily provided in a weatherproof enclosure, it is simpler to install for outdoor applications. However, since the NX4-60 is smaller in size, you could use it inside a building.

In a lightning prone or heavy lightning environment, the chances are greater to be hit by a severe surge; this environment is probably also more exposed to dry soil and poorer grounding conditions during some periods of the year. For these areas, Verint recommends to use NX4-60 model that will be able to divert to the grounding system a greater quantity of energy and present more chances to adequately protect the Ethernet equipment. The NX4-60 module gives a higher surge protection, but requires to be mounted in an appropriate waterproof electrical enclosure for outdoor applications (such as the Hammond 1554 Polycarbonate "2" series).

Both surge protection modules offer standard RJ-45 jacks for inbound and outbound termination. To install any of these modules, you need to cut and splice the outdoor Ethernet cable (with a weatherproof RJ-45 connector shell) provided with your purchase. For example:



The maximum length of the Ethernet connection with these surge protection modules installed is 75 meters.

Obviously, you must properly connect the S4300 device to the ground. Use a good grounding conductor and connect it to the ground lug on the S4300; make the connection to the ground system as short as possible. The grounding conductor should be a round cable with a minimum AWG 10 (2.6 mm) and maximum AWG 1 diameter, or the grounding wire that was provided with your protection module. On the S4300, the nearest grounding point is the pole itself.



## RF Contact between Masters

If the country of operation of your devices requires DFS compliance, you must ensure that the master devices (S4300 and S4100-R) in colocated cells “see” one another in their permanent location. Such a contact means that RF communication can be performed between each pair of masters, therefore preventing them to choose the same frequency channel. Using the same channel would cause interference between the colocated cells and reduce channel reliability and efficiency.

Apply the following procedure to ensure that *MasterA* sees *MasterB*. You will have to access the command line interface (CLI) of at least one master; for more information, see page 147.

### To ensure that two master devices see each other:

1. Take down the device name of MasterB.

This name is displayed in the Unit page of the Unit Configuration window in SConfigurator.

2. Shut down MasterB, then power it up.
3. Wait until MasterB has selected a frequency channel. To ensure that a channel is selected:
  - If MasterB is an S4300, go in the **Advanced > Communication Status and Statistics > Wireless Status** menu of the CLI. Wait until the value of Current SCF Connection Status is **Connected to X Clients and Y Slaves**.

```
*****
Advanced \ Communication Status and Statistics \ Wireless Status
-----
Parameters:
NIC Name           : AT5001 WIS CM6 A,B,G 2.4-5.8 GHz
NIC MAC Address    : 00-0B-6B-30-FA-42
Current Channel     : 56 (5280 MHz)
Current TX Rate     : 36 Mb/s
Current RX Rate     : 36 Mb/s
Average Signal Level : -53 dBm
Current SCF Connection Status: Connected to 1 Client and 0 Slave

RF Communication Quality : N/A
RF Margin                : N/A
Current EIRP              : 17 dBm
Maximum EIRP allowed     : 30 dBm
Indoor/Outdoor RF Regulation : Indoor/Outdoor FCCA FCC1

Commands:
1) Display link(s) Info
v) Visualize Last Site Survey Report
w) Initiate One-Time Site Survey
p) Previous Menu
*****
```

- If MasterB is an S4100, go in the **Connection Status** area of the Unit Wireless Configuration window (accessible through SConfigurator). Wait until the **Wireless** connection status is **Not Connected** or provides a communication quality; these statuses occur after **Radar Detection**.

Connection Status		
	Transmitter	Receiver
Wireless	-83 dBm, Excellent	

- If you do not have access to the connection status of MasterB and have automatic frequency channel selection, wait for the following time period: (starting order of MasterB - 1) multiplied by 80 seconds.
4. Perform a site survey in MasterA:
    - a. Open the CLI of the device.
    - a. Go in the **Advanced > Communication Status and Statistics > Wireless Status** menu.
    - b. Execute the **Initiate One-Time Site Survey** command.

- c. To see the progress of the operation, press **Enter** every second.

The site survey is completed when the value of Current SCF Connection Status returns to **Connected to X Clients and Y Slaves**, after having gone to **Site survey (100% completed)**.

- d. Execute the **Visualize Last Site Survey Report** command.
- e. Check that the MasterB name is listed as the Unit Name of one of the channels. You may need to scroll up the CLI window to see the beginning of the survey data.

For example, in the following site survey, MasterB has a visual connection with the MasterA device. If the MasterB name is not displayed in the site survey, it means that the two masters cannot see each other.

Last Site Survey Report, 4372 seconds old

Channel(1) Cost: 41						
Age	InterF.	Source MAC	Master MAC/	Rx	Unit Name/	
(s)	Type		802.11 BSSID	(dBm)	802.11 SSID	
-----						
11	SPCF MSTR	00-0B-6B-30-2A-46	00-0B-6B-30-2A-46	-54	MasterB	





# Reducing Wireless Interference

Wireless interference can be caused by:

- External sources
- Other Nextiva devices in colocated cells or on adjacent frequency channels

Follow specific guidelines to reduce interference as much as possible.

# Interference from External Sources

The 2.4 and 5 GHz frequency bands are license-free bands. This absence of frequency coordination can result in interference between various systems. For instance, if a link with an RF line of sight is subject to excessive video delay and very low frame rate (or possibly breakdown of video images), it could be due to interference. Fortunately, you have ways of adapting your setup to avoid interference:

- Change the frequency channel until you find a clean one.
- Replacing the integrated antenna with an external one producing a higher gain can significantly lower the interference from other radio systems and reduce the number of signals that are picked up. Consider replacing the antenna if switching channels does not correct the problem or if all channels must be used to colocate several systems.
- If installing an external antenna, choose horizontal polarization. Most external devices operating in the 2.4 or 5 GHz band use vertical polarization, as well as the integrated antennas in the Nextiva wireless devices. Using a different polarization can give a good isolation to external interferences caused by vertically polarized devices.

There should not be any interference in the 4.9 GHz band, since it is a licensed band with usage limited to public safety.

# Interference from Nextiva Devices

Wireless interference can occur between colocated wireless cells using adjacent frequency channels (for example, channels 149 and 153 in the 5 GHz band, or channels 1 and 6 in the 2.4 GHz band). The symptoms are lower throughput than expected or many CRC errors and communication retries; the number of CRC errors and retries is displayed in the command line interface of the device (Advanced > Communication Status and Statistics > Wireless Communication Throughput). A typical interference case is when many devices are installed on the same roof or share the same pole. Therefore, it is preferable to avoid using adjacent channels.

Even second adjacent channels can cause wireless interference.

If your setup requires the use of adjacent channels, follow these guidelines:

1. Separate as much as possible the devices from each other. See page 167 for the minimum distances to respect.
2. Vary antenna polarization. The integrated antenna uses vertical polarization, so when installing external antennas, select horizontal polarization. By reversing polarization, you improve the wireless cell isolation. If wireless cells share the same roof or pole, alternate antenna polarization.

**Note:** All the devices in a wireless cell must have the same polarization.

3. Perform a site survey to determine exactly which devices are causing interference. For the procedure, see page 163.
4. Decrease the tx power of the wireless links that have a good RF margin (15 dB or more). This way, the interference generated by the device is reduced.

5. Reduce the transmission (tx) bit rate of the cell affected by interference. The lower the tx bit rate, the better the resistance to interference.

## Performing a Site Survey

To reduce radio interference possibilities between two adjacent cells, the difference in signal level between the cells must not exceed a specific value that varies depending on the transmission (tx) bit rate used in the wireless cell:

<b>Tx Bit Rate</b>	<b>Maximum Signal Difference with the Adjacent Channel</b>	<b>Maximum Signal Difference with the Second Adjacent Channel</b>
54 Mbps	4 dB	14 dB
48 Mbps	10 dB	20 dB
36 Mbps	13 dB	23 dB
24 Mbps	15 dB	25 dB
18 Mbps	21 dB	31 dB
12 Mbps	21 dB	31 dB
9 Mbps	22 dB	32 dB
6 Mbps	23 dB	33 dB

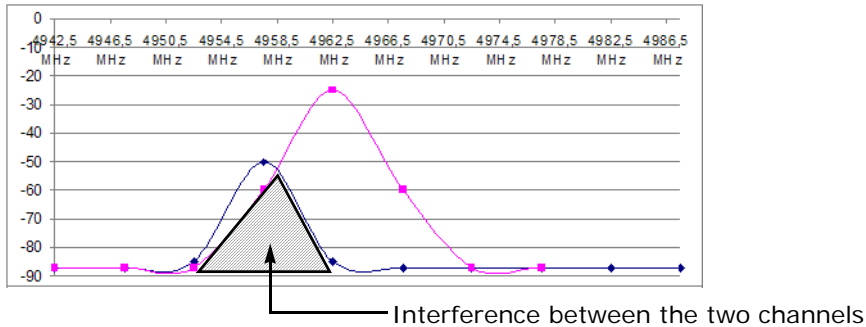
If the signal difference is higher than this maximum value, there will be too much interference in the adjacent cells. To calculate this signal difference, perform a site survey.

A site survey scans all frequency channels, evaluate the interference level in each channel, and allows you to choose the channel with the less interference.

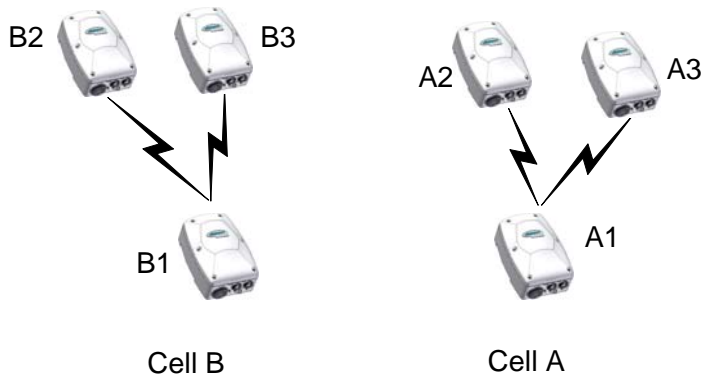
The following operations relative to RF site surveys are available:

- Specify the number of consecutive surveys to perform
- Start and stop a site survey
- Look at the last survey report
- Reset the survey database

Here is an example of a 23 dB signal difference between channels 8 and 9 in the 4.9 GHz band:



Consider the following setup in the 4.9 GHz band with 5-MHz bandwidth, where Cell B uses channel 6 and you are trying to add Cell A on channel 3 (adjacent to channel 6):



To determine if this setup is feasible, you need to conduct a site survey on device A1 (the master device in Cell A), then calculate the signal difference between the two cells. During the site survey, device A1 will find the other five devices. With the provided signal levels, you need to check if  $S2 - S1 \leq \text{Max}$ , where:

- S1 is the lowest signal level in the wireless cell of the device performing the site survey (A1 in the example).
- S2 is the highest signal level in the adjacent cell (Cell B in the example).
- Max is the maximum signal difference (23 dB for a 6 Mbps bit rate in the example).

**To calculate the emission signal difference between two adjacent wireless cells:**

1. Open SConfigurator, then click the **Units** tab.
2. Select the master device in the wireless cell you are adding, then click **Telnet**.

3. From the main menu of the command line interface (CLI), select **Advanced > Communication Status and Statistics > Wireless Status**, then press **Enter**.

```
*****
Advanced \ Communication Status and Statistics \ Wireless Status
-----
Parameters:
  NIC Name           : AT5006X DCMA-82 A,B,G 2.4,4.9,5.x GHz
  NIC MAC Address    : 00-0B-6B-2F-F8-E5
  Current Channel     : 7 (4950 MHz) 20 MHz channel bandwidth
  Current TX Rate     : 6 Mb/s
  Current RX Rate     : 6 Mb/s
  Average Signal Level : -65 dBm
  Current SCF Connection Status: Connected to 1 Client and 1 Slave

  RF Communication Quality : N/A
  RF Margin               : N/A
  Current EIRP            : 34 dBm
  Maximum EIRP allowed    : 42 dBm
  Indoor/Outdoor RF Regulation : Indoor/Outdoor FCCA FCC1
  1) Site survey iteration : 1

Commands:
1) Display link(s) Info
s) Start/Stop Site Survey
v) Visualize Last Site Survey Report
r) Reset Site Survey data base
p) Previous Menu
*****
```

4. For a thorough scan, specify 60 site survey iterations.
5. Start the site survey operation.

Note: During the execution, the RF link will be momentarily broken (duration varies depending on the number of iterations). The link is automatically restored when the survey is finished.

6. When the survey is complete, visualize the report. For example:

```

Last Site Survey Report, 53 seconds old
Channel(3) Cost: 48
Age  Interf.  Source MAC      Master MAC/      Rx  Unit Name/
(s)  Type      802.11 BSSID      (dBm) 802.11 SSID

-----
11 SPCF SLV  00-0B-6B-57-22-A9 00-0B-6B-2F-F8-E5 -75  Unit A2
11 SPCF SLV  00-0B-6B-2F-F9-3C 00-0B-6B-2F-F8-E5 -70  Unit A3
Channel(6) Cost: 35
Age  Interf.  Source MAC      Master MAC/      Rx  Unit Name/
(s)  Type      802.11 BSSID      (dBm) 802.11 SSID

-----
11 SPCF MSTR 00-0B-6B-57-22-14 00-0B-6B-2F-28-B8 -45  Unit B1
11 SPCF SLV  00-0B-6B-2F-09-DC 00-0B-6B-2F-28-B8 -60  Unit B3
11 SPCF SLV  00-0B-6B-2F-E9-88 00-0B-6B-2F-28-B8 -75  Unit B2
Channel(7) Cost: 0
Channel(8) Cost: 0
Channel(9) Cost: 0
Channel(10) Cost: 0
Channel(11) Cost: 0
Channel(12) Cost: 0
Channel(13) Cost: 0
Channel(16) Cost: 0
***** Cost Spectrum Image *****
Channel: 3 Cost-> 48 |>>>>>>>
Channel: 6 Cost-> 35 |>>>>>>>
Channel: 7 Cost-> 0 |
Channel: 8 Cost-> 0 |
Channel: 9 Cost-> 0 |
Channel: 10 Cost-> 0 |
Channel: 11 Cost-> 0 |
Channel: 12 Cost-> 0 |
Channel: 13 Cost-> 0 |
Channel: 16 Cost-> 0 |
***** Cost Spectrum Image *****

```

Diagram illustrating the mapping of channel data to device names and signal levels:

- Channel(3) Cost: 48
- Channel(6) Cost: 35
- Channel(7) Cost: 0
- Channel(8) Cost: 0
- Channel(9) Cost: 0
- Channel(10) Cost: 0
- Channel(11) Cost: 0
- Channel(12) Cost: 0
- Channel(13) Cost: 0
- Channel(16) Cost: 0

Devices found on channel 3:

- Unit A2
- Unit A3

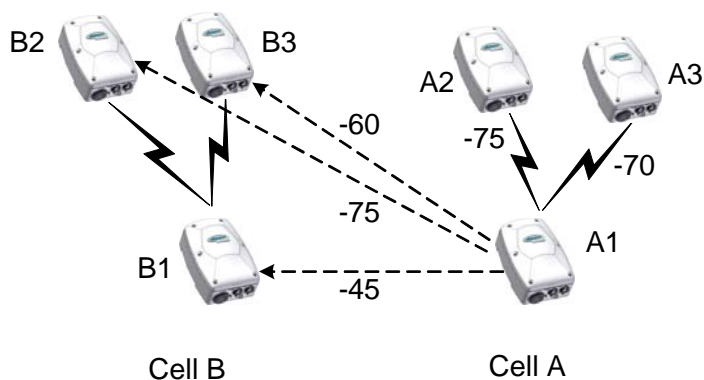
Devices found on channel 6:

- Unit B1
- Unit B3
- Unit B2

Device name

Signal level

The report provides the signal levels between device A1 and the other five devices in the network.

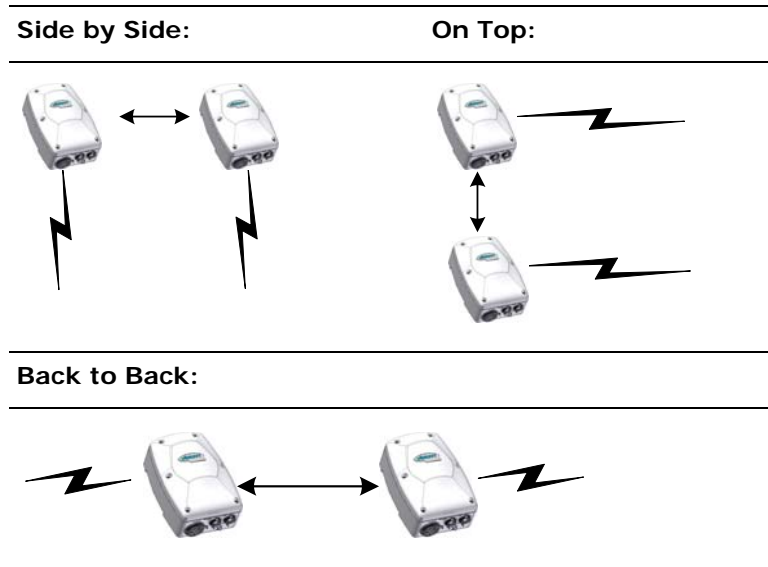


The lowest signal in Cell A is -75 (S1) and the highest signal in Cell B is -45 (S2). The result of  $S2 - S1$  ( $-45 - -75$ ) is 30. Since the signal difference is higher than 23 dB, there will be interference issues.

## Respecting Minimum Distances

To respect the maximum signal difference between two adjacent channels, you can use guidelines relative to minimum distances between the wireless devices. By respecting them, you can assume that there will be no radio interference between the devices.

Three physical setups are covered:



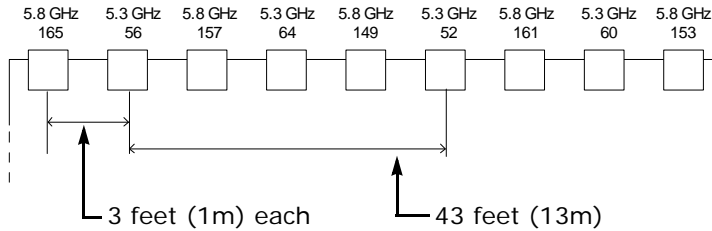
The minimum separation between devices using adjacent channels is, for a maximum signal difference of 25 dB:

Setup	5 GHz (12-dBi Antenna with 40° Beamwidth)	4.9 GHz (12-dBi Antenna with 40° Beamwidth)	2.4 GHz (8.5-dBi Antenna with 60° Beamwidth)
Side by side	43 feet (13m)	36.1 feet (11m)	55.8 feet (17m)
On top	13 feet (4m)	6.6 feet (2m)	6.2 feet (1.9m)
Back to back	7.8 feet (2.4m)	13.1 feet (4m)	15.7 feet (4.8m)

If you are using other antennas with narrower beamwidths, the distances may be reduced. For assistance, contact the customer service team.

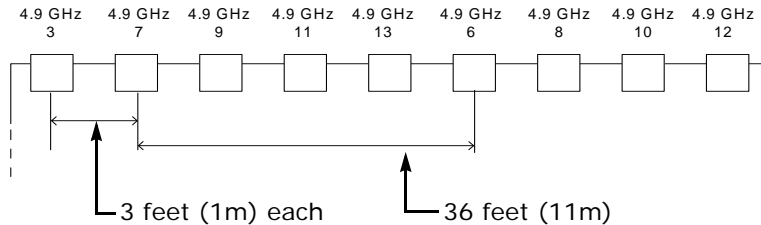
The following deployment scenarios respect these limitations:

- Using only 5 GHz channels, all on the same side of a building (Mexico and Europe only):



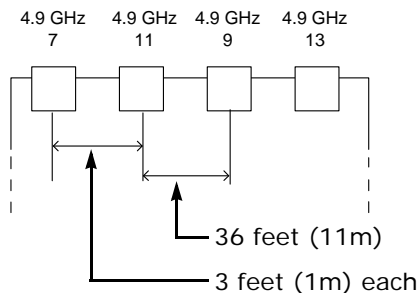
Notice that the devices using the adjacent channels 52 and 56 are separated by the prescribed 43 feet (13m). However, you can intersperse other devices in-between, as long as they do not use adjacent channels. This way, you can increase the device density without encountering interference problems.

- In the 4.9 GHz band, using only 5 MHz channels, all on the same side of a building:



Notice that the devices using the adjacent channels 7 and 6 are separated by the prescribed 36 feet (11m). However, you can intersperse other devices in-between, as long as they do not use adjacent channels. This way, you can increase the device density without encountering interference problems.

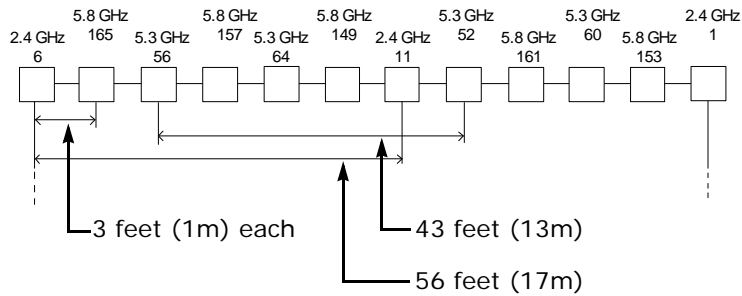
- In the 4.9 GHz band, using only 10 MHz channels, all on the same side of a building:



Since only four channels are available, it is unavoidable that two adjacent channels are positioned next to each other.



- Using 5 GHz and 2.4 GHz channels, all on the same side of a building (Mexico and Europe only):



The devices using the adjacent channels 6 and 11 in the 2.4 GHz are separated by the prescribed 56 feet (17m).



# Technical Specifications

Here are the S4300 technical specifications:

Network	RF interface	Proprietary SPCF
	RF bands	2.4 GHz 4.9 GHz 5 GHz
	Modulation	OFDM
	Encryption	128-bit AES
	Data rate (max. burst rate)	6, 9, 12, 18, 24, 36, 48, and 54 Mbps
	Ethernet connector	Weatherproof 10/100Base-T (RJ-45)
	Protocols	Transport: RTP/IP, UDP/IP, TCP/IP, or multicast IP Others: DNS and DHCP client
	Security	SSL-based authentication
Power	Input voltage	S4300, S4300-BR-PoE: 48V DC Power over Ethernet (PoE) 802.3af compliance S4300-BR, S4300-RP: 24V AC +/- 20% or 12V DC +/- 10%
	Maximum consumption	S4300, S4300-BR-PoE: PoE Class 3 (6.49 to 12.95W) S4300-BR, S4300-RP: 20W (1.6 A at 12V DC), 25 VA at 24V AC
Physical	Enclosure	NEMA 4X/IP 66 powder coat painted die-cast aluminum with wall-mount assembly
	Size	8.5D x 3.5H x 5.5W inches (217D x 90H x 138W mm)
	Weight	Casing: 3.3 lb (1.5 kg) Mounting assembly: 1.3 lb (0.6 kg)
	Environment	22°F to 122°F (-30°C to 50°C)
	Humidity	100% at 122°F (50°C)
Certification/ Regulation	General	RoHS compliant, UL certified

USA	FCC CFR47 Part 15 Subpart B, C, and E (15.247, 15.407, 15.107, 15.109) FCC Part 90 DSRC-C mask certification UL60950-1, First Edition
Canada	Industry Canada RSS-210, RSS-139, and ICES-003 CSA C22.2 NO. 60950-1, First Edition
Europe	CE marked ETSI EN 300 328 v1.7.1 (2006-10) ETSI EN 300 893 v1.3.1 (2005-08) ETSI EN 301 489-1 v1.7.1 (2007-04) ETSI EN 301 489-17 v1.3.2 (2007-06) IEC-60950-1, First Edition UL60950-1, First Edition

# Glossary

This glossary is common to the Nextiva line of edge device products.

**Access Point** A communication hub for connecting wireless edge devices to a wired LAN.

**AES** (Advanced Encryption Standard) An encryption standard used in the WPA2 authentication method.

**APIPA** (Automatic Private IP Addressing) A feature of Windows-based operating systems that enables a device to automatically assign itself an IP address when there is no Dynamic Host Configuration Protocol (DHCP) server available to perform that function. Also known as *AutoIP*.

**Bridge** See *Wireless Bridge*.

**CCTV** (Closed Circuit Television) A television system in which signals are not publicly distributed; cameras are connected to television monitors in a limited area such as a store, an office building, or on a college campus. CCTV is commonly used in surveillance systems.

**CIF** (Common Intermediate Format) A video format that easily supports both NTSC and PAL signals. Many CIF flavors are available, including CIF, QCIF, 2CIF, and 4CIF. Each flavor corresponds to a specific number of lines and columns per video frame.

**CLI** (Command Line Interface) A textual user interface in which the user responds to a prompt by typing a command.

**Codec** (Coder/Decoder) A software library that compresses or decompresses a video stream following a specific protocol.

**Configuration Assistant** A proprietary graphical program used to configure and update the firmware of the S1100 edge devices.

**Decoder** See *Receiver*.

**DHCP** (Dynamic Host Configuration Protocol) A communication protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in a network.

**DVR** (Digital Video Recorder) A device (usually a computer) that acts like a VCR in that it has the ability to record and play back video images. The DVR takes the feed from a camera and records it into a digital format on a storage device which is most commonly the hard drive.

**Edge Device** A Nextiva device transmitting or receiving video signals through an IP network. The devices can be wireless or wired; some transmitters are IP cameras.

**Encoder** See *Transmitter*.

**Ethernet** A local area network (LAN) architecture using a bus or star topology and supporting data transfer rates of 10, 100, and 1000 Mbps. It is one of the most widely implemented LAN standards. The 802.11 protocols are often referred to as "wireless Ethernet."

**Firmware** Software stored in read-only memory (ROM) or programmable ROM (PROM), therefore becoming a permanent part of a computing device.

**IP** (Internet Protocol) The network layer for the TCP/IP protocol suite widely used on Ethernet networks.

**LAN** (Local Area Network) A computer network that spans a relatively small area. A LAN can connect workstations, personal computers, and surveillance equipment (like edge devices). See also *WAN*.

**MPEG-4** A graphics and video lossy compression algorithm standard that is derived from MPEG-1, MPEG-2, and H.263. MPEG-4 extends these earlier algorithms with synthesis of speech and video, fractal compression, computer visualization, and artificial intelligence-based image processing techniques.

**Multicast** Communication between a sender and multiple receivers on a network; the devices can be located across multiple subnets, but not through the Internet. Multicast is a set of protocols using UDP/IP for transport.

**NTSC** (National Television Standards Committee) The North American standard (525-line interlaced raster-scanned video) for the generation, transmission, and reception of television signals. In addition to North America, the NTSC standard is used in Central America, a number of South American countries, and some Asian countries, including Japan. Compare with *PAL*.

**NTP** (Network Time Protocol) A protocol designed to synchronize the clocks of devices over a network.

**OSD** (On-screen Display) Status information displayed on the video monitor connected to a receiver edge device.

**PAL** (Phase Alternation by Line) A television signal standard (625 lines) used in the United Kingdom, much of western Europe, several South American countries, some Middle East and Asian countries, several African countries, Australia, New Zealand, and other Pacific island countries. Compare with *NTSC*.

**PEAP** (Protected Extensible Authentication Protocol) A method to securely transmit authentication information, including passwords, over a wireless network.

**Point-to-Point Connection** The association of a transmitter and a receiver to view video coming from an analog camera on an analog monitor.

**PSK** (Pre-Shared Key) A mode of the WPA and WPA2 security protocols, designed for home and small office networks that cannot afford the cost and complexity of an authentication server. It is also known as *personal mode*.

**PTL** (Push-To-Listen) In a two-way system, the communication mode in which the listener must push a button while listening.

**PTT** (push-To-Talk) In a two-way system, the communication mode in which the talker must push a button while talking.

**PTZ Camera** (Pan-Tilt-Zoom) An electronic camera that can be rotated left, right, up, or down as well as zoomed in to get a magnified view of an object or area. A PTZ camera monitors a larger area than a fixed camera.

**QoS** (Quality of Service) A set of low-level networking protocols giving higher priority to more important data flows while ensuring that the less important ones do not fail.

**Receiver** A device converting a digital video signal into an analog form. Also called *decoder*.

**Repeater** A range extender for wireless links.

**RF** (Radio Frequency) Any frequency within the electromagnetic spectrum associated with radio wave propagation. When a modulated signal is supplied to an antenna, an electromagnetic field is created that is able to propagate through space. Many wireless technologies are based on RF field propagation.

**RS-232** A standard interface approved by the Electronic Industries Alliance (EIA) for connecting serial devices.

**RS-422** A standard interface approved by the Electronic Industries Alliance (EIA) for connecting serial devices, designed to replace the older RS-232 standard because it supports higher data rates and greater immunity to electrical interference.

**RS-485** An Electronics Industry Alliance (EIA) standard for multipoint communications.

**SConfigurator** A proprietary graphical program used to configure and update the firmware of edge devices.

**Serial Port** An interface that can be used for serial communication, in which only one bit is transmitted at a time. A serial port is a general-purpose interface that can be used for almost any type of device.

**SSL** (Secure Sockets Layer) A commonly used protocol for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. The SSL protocol secures the following data: I/O, serial port, and VSIP communication; it does not apply to audio and video transmission.

**TKIP** (Temporal Key Integrity Protocol) A security protocol used in the WPA authentication method.

**TLS** (Transport Layer Security) A cryptographic protocol that provide secure communications on a wireless network.

**Transceiver** (Transmitter/Receiver) A device that both transmits and receives analog or digital signals.

**Transmitter** A device sending video signals captured with a connected camera to a receiver. The transmitter converts the analog signal into a digital form before transmitting it. Also called *encoder*.

**TTLS** (Tunneled Transport Layer Security) A cryptographic protocol that creates a secure TLS tunnel.

**VSIP** (Video Services over IP) A proprietary communication protocol for sending messages between a computer and a Nextiva edge device, or between two devices.

**WAN** (Wide Area Network) A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs).

**WEP** (Wired Equivalent Privacy) A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. It is designed to afford wireless networks the same level of protection as a comparable wired network.

**Wireless Bridge** A link between two networks, wired or wireless.

**Wireless Cell** A group of wireless devices that communicate together on the same radio frequency channel and share the same wireless passkey.

**Wireless Transmission** A technology in which electronic devices send information to receivers using radio waves rather than wiring.

**WPA** (Wi-Fi Protected Access version 1) An authentication method to secure wireless systems. It is the successor of WEP. WPA implements the majority of the IEEE 802.11i standard.



**WPA2** (Wi-Fi Protected Access version 2) An authentication method that implements the full 802.11i standard, but will not work with some older network cards. It is also known as *802.11i*.

# Index

## Numerics

- 0.6 F1 37
- 12V DC 57
- 2.4 GHz frequency band. *See* frequency band.
- 24V AC 57
- 4.9 GHz frequency band. *See* frequency band.
- 5 GHz frequency band. *See* frequency band.
- 802.11a. *See* frequency band.
- 802.11g. *See* frequency band.

## A

- abnormal power-up condition 147
- access management 125
- access point application
  - configuration 41–47
  - defined 23
  - installation 48–52
- account, user 125
- address, IP. *See* IP address.
- adjacent channel 33, 162–169
- administrator account 125
- allocation of frequency bands 15
- antenna
  - certified 184
  - choosing 38
  - gain 38, 45, 132, 184
  - installation 52
  - integrated 2
  - location, for Fresnel zone 37
  - requirements 38
  - reversing polarization 162
  - separation, in colocated systems 29, 167
- APIPA addressing scheme 152
- application types 22–27

## B

- band, frequency. *See* frequency band.
- bandwidth, channel 14, 132
- bit rate
  - dynamic 19
  - RF 132
  - video 18
- boot sequence in DFS 20
- bridge application, wireless
  - configuration 55
  - defined 26
  - installation 65

## C

- cable
  - Ethernet. *See* Ethernet cable.
  - power 5, 57
- casing of the device 6
- cell, wireless. *See* wireless cell.
- certification, wireless 183
- certificate, SSL 3
- channel bandwidth 132
- channel, RF
  - available 13
  - in colocated cells 29
  - fragmenting 14, 132
  - reduced set of 33
  - selecting 20, 45, 131, 149
- characteristics of the device 2
- CLI (command line interface) 126, 147
- cold weather 145
- colocated cell 29–36
- common VSIP port 143
- communication between master and slaves 47
- compatibility of firmware versions 17
- compliance 57, 183
- computer requirements 11
- computer, changing the IP address 74
- configuration
  - default 139, 144, 150
  - order, in the wireless cell 17
  - web interface 124–138
- connection
  - 12V DC 57
  - 24V AC 57
  - PoE 40
- constraints in Europe 20–22, 32–36
- contact between two masters 32, 158–160
- country
  - available frequency bands per 15
  - certified antennas for 184
  - selecting 133

## D

- data throughput 18
- default configuration 139, 144, 150
- detecting duplicate masters 143
- detection of radars 20, 33, 134
- DFS (Dynamic Frequency Selection)
  - boot sequence 20–22
  - defined 15
  - setups in Europe 32–36
- DHCP (Dynamic Host Configuration Protocol) 43, 129

- dimensions of the device 7
- distance
  - between antennas 29, 167
  - between antennas and persons 38
  - between colocated devices 29, 167
- downgrade of firmware 143
- DSCP (Differentiated Service Code Points) 149
- duplicate IP address 42
- duplicate master detection 143
- dynamic bit rate control 19
- Dynamic Frequency Selection. *See* DFS (Dynamic Frequency Selection).

## E

- EIRP 38, 184
- enclosure of the device 6
- Ethernet cable
  - for configuration 58
  - maximum length 56, 58
  - supplied 3
- Ethernet network LED 145
- ETSI (European Telecommunications Standards Institute) 15
- Europe
  - colocation in the 2.4 GHz band 31–32
  - colocation in the 5 GHz band 32–36
  - DFS context 15, 20–22
  - TPC context 15, 20
- evaluating the location 36
- exposure, RF 38
- external antenna. *See* antenna.

## F

- factory default configuration 139, 144, 150
- failover of masters 28
- false radar detection 33
- features of the device 2
- finding a lost device 143
- firmware update
  - ActiveX control for 121
  - downgrading 143
  - performing 139, 143
  - preventing 126, 127
  - without losing devices 17
- first Fresnel zone 37
- frequency band
  - available 13
  - certified antennas for 184
  - distance limitations 167
  - licensed 13
  - public safety 13
  - selecting 131

- frequency channel
  - available 13
  - in colocated cells 29
  - fragmenting 14, 132
  - reduced set of 33
  - selecting 20, 45, 131, 149
- Fresnel zone 37

## G

- gain of antenna 38, 45, 132, 184
- gateway 130
- global security profile 127
- GMT (Greenwich Mean Time) 136

## H

- half channel selection 33
- hidden node problem 3
- HTTP access 126
- HTTP settings for the web interface 138
- HTTPS access 126

## I

- identifying a device 145
- indoor/outdoor RF regulation 135
- injector, PoE 40
- installation
  - antenna. *See* antenna.
  - device. *See the device entries.*
- integrated antenna 2
- interference, RF 161
- IP address
  - APIPA 152
  - changing, for the computer 74
  - duplicate 42
  - setting 43, 129
  - temporary 152
- IP camera with wireless bridge 26, 55

## L

- LAN LED 145
- LED 7, 144–147
- length of Ethernet cable 56, 58
- licensed band. *See* frequency band.
- limitations
  - colocated systems 29
  - distance 29, 167
  - Europe 20–22, 32–36
- line-of-sight path 36
- loading default configuration 139, 144, 150
- location evaluation 36
- lost device 143

## M

- MAC mode 3, 131
- MAC role 16, 131
- maintenance 139
- margin
  - minimum RF 134
- mask, subnet 129
- master
  - boot sequence with DFS 21
  - communication with slaves 47
  - defined 16, 131
  - duplicate 143
  - ensuring RF contact 32, 158–160
  - redundant 28
- maximum EIRP 38, 184
- maximum gain of antenna 38, 184
- maximum length of Ethernet cable 56, 58
- maximum number of devices in a cell 18
- maximum transmission power. *See* transmission power.
- Media Access Control (MAC). *See the "MAC" entries.*
- minimum RF margin 134
- mounting angles 7
- mounting assembly 48
- multicast data transfer 135

## N

- name of device 136
- network
  - planning 12–27
  - settings 42, 129
- NTP (Network Time Protocol) 136

## O

- omni-directional antenna 52, 70, 89, 104, 119
- order in the configuration and update process 17
- order, starting 21, 45, 134

## P

- passkey
  - SSL 127
  - for Telnet connection 125
  - for web interface 125
  - wireless. *See* wireless passkey.
- planning
  - RF 36–38
  - wireless cell 20–27
- PoE (power-over-Ethernet) injector 40
- point-to-multipoint repeater
  - configuration 92–98
  - defined 24
  - installation 99–103

- point-to-multipoint wireless bridge
  - defined 26, 55
- point-to-point repeater
  - configuration 74–83
  - defined 25
  - installation 84–88
- polarization, antenna 162
- power cable 5, 57
- power supply requirements 57
- power, transmission. *See* transmission power.
- power-over-Ethernet (PoE) injector 40
- power-up condition, abnormal 147
- preventing access 126
- protection
  - device configuration 126
  - surge 52, 154
- protocol, MAC 3, 131
- public safety band. *See* frequency band.

## Q

- Quality of Service (QoS) 149

## R

- radar detection 20, 33, 134
- radio frequency. *See* RF (radio frequency).
- rebooting the device 139, 144
- redundant master 28
- repeater
  - point-to-multipoint 24, 91
  - point-to-point 25, 73
  - wireless bridge 27, 106
- requirements
  - antenna 38
  - computer 11, 41
  - power supply 57
- reset to factory default 139, 150
- RF (radio frequency)
  - channel. *See* frequency channel.
  - contact between two masters 32, 158–160
  - exposure considerations 38
  - global spectrum allocation 15
  - LED 145
  - line of sight 36
  - parameters. *See* wireless parameters.
  - planning 36–38
  - See also the "wireless" entries.*
- RF margin, minimum 134
- RoHS 192
- role of device 131
- rotation positions of the device 7

**S**

- S4100
  - compatibility with S4300 17
  - maximum number in a cell 18
  - role in a wireless cell 16, 25
- S4200
  - checking communication with master 47
  - compatibility with S4300 17
  - maximum number in a cell 18
  - role in a wireless cell 16, 23
- S4300
  - in an access point application 23
  - configuration 41–47
  - installation 48–52
- S4300-BR
  - configuration 58–65
  - installation 65–70
  - in a wireless bridge application 26
- S4300-RP
  - configuration 74–83, 92–98, 107–113
  - installation 84–88, 99–103, 114–118
  - in a point-to-multipoint repeater 24, 91
  - in a point-to-point repeater 25, 73
  - in a wireless bridge repeater 27, 106
- SConfigurator 42–47, 58–65, 78–83, 93–98, 108–113
- SDCF 131
  - security
    - for the device 126, 3
    - for wireless data 131
- sensitivity threshold 134
- separation between antennas 167
- sequence of boot in DFS 20
- setups in Europe 34–36
- signal difference between adjacent channels 163
- site survey 149, 159, 163
- slave
  - boot sequence with DFS 22
  - communication with master 47
  - defined 16, 131
  - maximum number in a cell 18
- SPCF 3, 131
- specifications, technical 170
- spectrum allocation 15
- SSL (Secure Sockets Layer) 3, 127
- starting order 21, 45, 134
- status LED 146
- status of the device 128
- subnet mask 129
- sun shield 52
- surge protection 52, 154
- survey, site 149, 159, 163
- system planning 20–27
- system status 128
- system time 136

**T**

- technical specifications 170
- Telnet
  - accessing the CLI 147
  - preventing access 126
- temporary IP address 152
- throughput, data 18
- tilt positions of the device 7
- time, system 136
- ToS (Type of Service) 149
- TPC (Transmit Power Control) 15, 20
- transmission power
  - reducing, for TPC 20
  - setting 134
- troubleshooting 144

**U**

- user account 125

**V**

- Verint web site vii
- VSIP port 136, 143
- VSIP settings 135

**W**

- warmup period 145
- web client account 125
- web interface
  - accessing with a password 125
  - after a firmware update 121
  - for configuration 124–138
  - HTTP settings 138
  - maintaining the device with 139
  - opening 122
  - preventing access 126
  - secure access 127
- web site, Verint vii
- width, channel 14, 132
- wireless bridge
  - configuration 58–65
  - defined 26
  - installation 65–70
- wireless bridge repeater
  - configuration 107–113
  - defined 27
  - installation 114–118
- wireless cell 16, 20–27
- wireless certification 183
- wireless Ethernet LED 145
- wireless frequency plan 15
- wireless parameters 44–47, 61–65, 80–83, 95–98, 110–113, 130–135

- wireless passkey
  - in an access point 46
  - in colocated cells 29
  - in a point-to-multipoint repeater 97
  - in a point-to-point repeater 82
  - in a single cell 16
  - in the web interface 131
  - in a wireless bridge 64
  - in a wireless bridge repeater 112

# Compliance

The S4300 series wireless device is RoHS compliant and UL certified. It is also certified to be used in the following countries:

- USA
- Canada
- Mexico
- CE countries using the harmonized bands

Note: The S4300 series devices require professional installation. They should be installed in a location that would prevent the general population from approaching from 3 feet (1 meter) of the radiating element. You must use only antennas certified by Verint.

# USA

Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation of the device.

This equipment has been tested and found to comply with the limits for Class B Digital Device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in residential installation. This equipment generates and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the S4300 device
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Any changes or modifications not expressly approved by Verint Systems Inc. could void the user's authority to operate the equipment.

The compliance information for this country is:

	2.4 to 2.472 GHz	4.940 to 4.990 GHz	5.725 to 5.825 GHz
FCC identifier	VKHS4X00DCMA82	VKHS4X00DCMA82	VKHS4X00DCMA82
FCC certifications	47 CFR part 15 subpart B (15.107, 15.109)	47 CFR part 15 subpart B (15.107, 15.109)	47 CFR part 15 subpart B (15.107, 15.109)
	47 CFR part 15 subpart C (15.247)	47 CFR part 90	47 CFR part 15 subpart C (15.247)
Radio	DCMA-82 HI	DCMA-82 HI	DCMA-82 HI



	2.4 to 2.472 GHz	4.940 to 4.990 GHz	5.725 to 5.825 GHz
<p>Certified antennas</p> <p>The indicated tx power is generated by the device with the specified antenna.</p>	<p>Integrated tri-band Verint antenna: 2.4 GHz with 8.5 dBi gain and 13 dBm tx power</p> <p>ANT-WP16-24/S: Patch antenna with 15.5 dBi gain and 10 dBm tx power</p>	<p>ANT-WP8-49/5x: Omni-directional antenna with 8 dBi and 23 dBm tx power</p> <p>Integrated tri-band Verint antenna: 4.9 GHz with 12 dBi gain and 20 dBm tx power</p> <p>ANT-WP18-49: Linear, flat-panel antenna with 18 dBi gain and 20 dBm tx power</p> <p>ANT-WP25-49: Linear, flat-panel antenna with 25 dBi gain and 20 dBm tx power</p>	<p>ANT-WP8-49/5x: Omni-directional antenna with 8 dBi and 23 dBm tx power</p> <p>Integrated tri-band Verint antenna: 5.x GHz with 12 dBi gain and 23 dBm tx power</p> <p>ANT-WS16-5x/S: Patch 90-degree antenna with 16 dBi gain and 20 dBm tx power</p> <p>ANT-WP19-5x/S: Patch antenna with 19 dBi gain and 17 dBm tx power</p> <p>ANT-WP23-5x/S: Patch antenna with 23 dBi gain and 12 dBm tx power</p> <p>The 19 dBi and 23 dBi antennas can use the full tx power (23 dBm) in point-to-point systems. The antennas must be installed by certified professionals only.</p>
Rule summary	<p>Band is for indoor/outdoor.</p> <p>Max EIRP:</p> <ul style="list-style-type: none"> <li>■ 36 dBm</li> <li>■ Point-to-point system: 53 dBm</li> </ul>	<p>Band is for indoor/outdoor.</p> <p>Max EIRP:</p> <ul style="list-style-type: none"> <li>■ 5 MHz width: 27 dBm and 27 dBi for fixed system</li> <li>■ 10 MHz width: 30 dBm and 27 dBi for fixed system</li> <li>■ 20 MHz width: 33 dBm and 27 dBi for fixed system</li> </ul>	<p>Band is for indoor/outdoor.</p> <p>Max EIRP:</p> <ul style="list-style-type: none"> <li>■ 36 dBm</li> <li>■ Point-to-point system: 53 dBm</li> </ul>

# Canada

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

The compliance information for this country is:

	2.4 to 2.472 GHz	4.940 to 4.990 GHz	5.725 to 5.825 GHz
IC identifier	7286A-S4X0082	7286A-S4X0082	7286A-S4X0082
Radio	DCMA-82 HI	DCMA-82 HI	DCMA-82 HI
Certified antennas The indicated tx power is generated by the device with the specified antenna.	Integrated tri-band Verint antenna: 2.4 GHz with 8.5 dBi gain and 13 dBm tx power  ANT-WP16-24/S: Patch antenna with 15.5 dBi gain and 10 dBm tx power	ANT-WP8-49/5x: Omni-directional antenna with 8 dBi and 23 dBm tx power  Integrated tri-band Verint antenna: 4.9 GHz with 12 dBi gain and 20 dBm tx power  ANT-WP18-49: Linear, flat-panel antenna with 18 dBi gain and 20 dBm tx power  ANT-WP25-49: Linear, flat-panel antenna with 25 dBi gain and 20 dBm tx power	ANT-WP8-49/5x: Omni-directional antenna with 8 dBi and 23 dBm tx power  Integrated tri-band Verint antenna: 5.x GHz with 12 dBi gain and 23 dBm tx power  ANT-WS16-5x/S: Patch 90-degree antenna with 16 dBi gain and 20 dBm tx power  ANT-WP19-5x/S: Patch antenna with 19 dBi gain and 17 dBm tx power  ANT-WP23-5x/S: Patch antenna with 23 dBi gain and 12 dBm tx power  The 19 dBi and 23 dBi antennas can use the full tx power (20 dBm) in point-to-point systems. The antennas must be installed by certified professionals only.

	2.4 to 2.472 GHz	4.940 to 4.990 GHz	5.725 to 5.825 GHz
Rule summary	<p>Band is for indoor/outdoor.</p> <p>Max EIRP:</p> <ul style="list-style-type: none"> <li>■ 36 dBm</li> <li>■ Point-to-point system: 53 dBm</li> </ul>	<p>Band is for indoor/outdoor.</p> <p>Max EIRP:</p> <ul style="list-style-type: none"> <li>■ 5 MHz width: 27 dBm and 27 dBi for fixed system</li> <li>■ 10 MHz width: 30 dBm and 27 dBi for fixed system</li> <li>■ 20 MHz width: 33 dBm and 27 dBi for fixed system</li> </ul>	<p>Band is for indoor/outdoor.</p> <p>Max EIRP:</p> <ul style="list-style-type: none"> <li>■ 36 dBm</li> <li>■ Point-to-point system: 53 dBm</li> </ul>

# Mexico

The compliance information for the 2.4 and 4.9 GHz bands for this country is:

	2.4 to 2.472 GHz	4.940 to 4.990 GHz
Standard		Need special approval from COFETEL
Radio	DCMA-82 HI	DCMA-82 HI
Certified antennas The indicated tx power is generated by the device with the specified antenna.	Integrated tri-band Verint antenna: 2.4 GHz with 8.5 dBi gain and 13 dBm tx power  ANT-WP16-24/S: Patch antenna with 15.5 dBi gain and 10 dBm tx power	ANT-WP8-49/5x: Omni-directional antenna with 8 dBi and 23 dBm tx power  Integrated tri-band Verint antenna: 4.9 GHz with 12 dBi gain and 20 dBm tx power  ANT-WP18-49: Linear, flat-panel antenna with 18 dBi gain and 20 dBm tx power  ANT-WP25-49: Linear, flat-panel antenna with 25 dBi gain and 20 dBm tx power
Rule summary	Band is for indoor/outdoor. Max EIRP: <ul style="list-style-type: none"> <li>■ 30 dBm</li> <li>■ Pt-to-pt system: 33 dBm</li> </ul>	Band is for indoor/outdoor. Max EIRP: <ul style="list-style-type: none"> <li>■ 5 MHz width: 27 dBm and 27 dBi for fixed system</li> <li>■ 10 MHz width: 30 dBm and 27 dBi for fixed system</li> <li>■ 20 MHz width: 33 dBm and 27 dBi for fixed system</li> </ul>

The compliance information for the 5 GHz bands for this country is:



	5.15 to 5.25 GHz	5.25 to 5.35 GHz	5.725 to 5.825 GHz
Standard	Resolution 229 of the UIT  Regulation: UIT-R M.1450-2 and UIT-R F.1244	Resolution 229 of the UIT  Regulation: UIT-R M.1450-2 and UIT-R F.1244	Resolution 229 of the UIT  Regulation: UIT-R M.1450-2 and UIT-R F.1244
Radio	DCMA-82 HI	DCMA-82 HI	DCMA-82 HI

	5.15 to 5.25 GHz	5.25 to 5.35 GHz	5.725 to 5.825 GHz
<p>Certified antennas</p> <p>The indicated tx power is generated by the device with the specified antenna.</p>	<p>ANT-WP8-49/5x: Omni-directional antenna with 8 dBi and 23 dBm tx power</p> <p>Integrated tri-band Verint antenna: 5.x GHz with 12 dBi gain and 11 dBm tx power</p>	<p>ANT-WP8-49/5x: Omni-directional antenna with 8 dBi and 23 dBm tx power</p> <p>Integrated tri-band Verint antenna: 5.x GHz with 12 dBi gain and 18 dBm tx power</p>	<p>ANT-WP8-49/5x: Omni-directional antenna with 8 dBi and 23 dBm tx power</p> <p>Integrated tri-band Verint antenna: 5.x GHz with 12 dBi gain and 23 dBm tx power</p> <p>ANT-WS16-5x/S: Patch 90-degree antenna with 16 dBi gain and 20 dBm tx power</p> <p>ANT-WP19-5x/S: Patch antenna with 19 dBi gain and 17 dBm tx power</p> <p>ANT-WP23-5x/S: Patch antenna with 23 dBi gain and 12 dBm tx power</p>
Rule summary	<p>Band is for indoor/outdoor.</p> <p>Max EIRP: 23 dBm</p>	<p>Band is for indoor/outdoor.</p> <p>Max EIRP: 30 dBm</p>	<p>Band is for indoor/outdoor.</p> <p>Max EIRP: 36 dBm</p>

## Europe

The CE countries using the harmonized bands are: Austria, Belgium, Bulgaria, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Lithuania, Luxembourg, Netherland, Norway, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, and United Kingdom.

The compliance information for these countries is:

	2.4 to 2.472 GHz	5.25 to 5.35 GHz	5.47 to 5.725 GHz
Certifications	EN 300 328-2 (article 3.2 of R&TTE directive WLAN 2.4 GHz)  EN 301 489-1 (article 3.1b of R&TTE directive EMC emissions)	EN 301 893 (article 3.2 of R&TTE directive)  EN 301 489-1 (article 3.1b of R&TTE directive EMC emissions)	EN 301 893 (article 3.2 of R&TTE directive)  EN 301 489-1 (article 3.1b of R&TTE directive EMC emissions)
Radio	DCMA-82 HI	DCMA-82 HI	DCMA-82 HI
Certified antennas  The indicated tx power is generated by the device with the specified antenna.	Integrated tri-band Verint antenna: 2.4 GHz with 8.5 dBi gain and 11 dBm tx power	ANT-WP8-49/5x: Omni-directional antenna with 8 dBi and 23 dBm tx power  Integrated tri-band Verint antenna: 5.x GHz with 12 dBi gain and 8 dBm tx power	ANT-WP8-49/5x: Omni-directional antenna with 8 dBi and 23 dBm tx power  Integrated tri-band Verint antenna: 5.x GHz with 12 dBi gain and 15 dBm tx power
Rule summary	Band is for indoor/outdoor. Max EIRP: 20 dBm   CE! France, Monaco: Outdoor restricted to channels 1 to 7.  CE! Greece, Italy, Spain: Outdoor needs license.  CE! Belgium: An outdoor link greater than 300m requires notification to spectrum agency.	Band is for indoor only. DFS/TPC is needed. Max EIRP: 27 dBm	Band is for indoor/outdoor. DFS/TPC is needed. Max EIRP: 27 dBm   CE! Greece, Italy: Outdoor needs license.

## Declaration of Conformity

**Manufacturer:**

Verint Systems Inc.  
1800 Berlier  
Laval, Québec  
H7L 4S4  
Canada

**Declares under sole responsibility that the product:**

Product name: Outdoor wireless device  
Model number: S4300-CE, S4300-BR-CE, and S4300-RP-CE

**To which this declaration relates is in conformity with the following standards or other documents:****R&TTE Directive 1999/5/EC**

ETSI EN 300 328 v1.7.1 (2006-10)  
ETSI EN 300 893 v1.3.1 (2005-08)  
ETSI EN 301 489-1 v1.7.1 (2007-04)  
ETSI EN 301 489-17 v1.3.2 (2007-06)  
IEC-60950-1, First Edition

Verint hereby declares that the equipment specified above conforms to the above Directive(s) and Standard(s).

October 17th, 2007  
Laval, Canada

For the official signed declaration of conformity, visit <http://www.verint.com/certifications>.

# RoHS Declaration of Compliance

Verint believes in the importance of conducting our business in a manner that will help protect the environment as well as our employees, customers, and the public.

To that end, we are committed to bringing our existing and future product lines into EU RoHS Directive compliance.

Thus, as of July 1 2006, the following products, S4300, S4300-BR, S4300-RP, S4300-CE, S4300-BR-CE, and S4300-RP-CE, will comply with the DIRECTIVE 2002/95/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 January 2003 (RoHS) regarding the restriction of the use of certain hazardous substances in electrical and electronic equipment.

The S4300, S4300-BR, S4300-RP, S4300-CE, S4300-BR-CE, and S4300-RP-CE products will not exceed the maximum concentrations of 0.1% by weight in homogenous materials for lead, hex chrome, mercury, PBB, PBDE, and 0.01% for cadmium. In addition, the S4300, S4300-BR, S4300-RP, S4300-CE, S4300-BR-CE, and S4300-RP-CE products will qualify for the "lead in servers solders" exemption as set forth in the Directive.

This declaration is provided based on reasonable inquiry of our suppliers and represents our actual knowledge based on the information provided by our suppliers.





POWERING ACTIONABLE INTELLIGENCE®

---

## AMERICAS

[info@verint.com](mailto:info@verint.com)

[www.verint.com/videosolutions](http://www.verint.com/videosolutions)

## EMEA

[marketing.emea@verint.com](mailto:marketing.emea@verint.com)

[www.verint.com/videosolutions](http://www.verint.com/videosolutions)

## APAC

[marketing.apac@verint.com](mailto:marketing.apac@verint.com)

[www.verint.com/videosolutions](http://www.verint.com/videosolutions)